Cryptocurrencies and Beyond: Using Design Science Research to Demonstrate Diverse Applications of Blockchains

Steven Huckle

Department of Informatics

University of Sussex

This dissertation is submitted for the degree of *Doctor of Philosophy*

December, 2019

Declaration

I hereby declare that, except where I make specific reference to the work of others, the contents of this thesis are original. Indeed, unless I specify that some text in this thesis includes collaborative work, the work contained herein is mine alone.

Furthermore, this work has not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university.

Steven Huckle

December, 2019

I dedicate this thesis to all beings. These are uncertain times; may you be safe.

Acknowledgement

My career in computing began back in 1992 when I completed a Youth Training Scheme (YTS) in COBOL Programming. That led to my employment as a Junior Programmer, which eventually fast-tracked me onto a degree at the University of North London (UNL). Several people gave up their time to help my development then. Without them, there is a good chance this thesis would never have happened because it is the culmination of a career that might never have materialised without those early influences. That includes the tutors on that YTS scheme, who encouraged me to go way beyond the remit of the course. It includes the over-worked IT Manager at my first job, who allowed me to 'play' on an ICL DRS6000 and its UNIX operating system. The skills I learned then remain relevant. It includes the Head of the Computing Department at UNL, who offered me a place on the Computer Science course, even though I failed (marginally) the entrance exam. To my shame, I cannot remember a single one of their names. However, they all have my humble gratitude for believing in me. I hope this thesis proves you were right.

I am also immensely grateful to my great friend Nick, who introduced me to Bitcoin back when it was still profitable to mine it at my home.

Several people had a direct influence on this thesis. First and foremost is my PhD Supervisor, Dr Martin White. I remain unaware of whether he intended me to orient this work entirely around design science research, but he kept mentioning the phrase, so when it dawned on me, eventually, that I should go and research the term, it proved the pivotal moment. Then there is my second Supervisor, Dr Natalia Beloff, whose words of wisdom enabled me to keep this work in scope. Next is Dr Phil Watten, who made the effort to critique an early draft of this work. The result was his wise suggestion that I make much more of a paragraph focused on an idea for a cryptocurrency. That input proved important. Finally, there is Dr David Rozas, a Researcher with the P2P Models team, at the Universidad Complutense de Madrid. David and I worked on a paper that discusses the commons-based peer production (CBPP) practices of the community behind

the open-source software website content management system, Drupal. CBPP is infused throughout this work, so David's knowledge there proved invaluable. Thank you so much to all of you.

Thank you to Patrick, Coby and Richard, who had the displeasure of sharing an office with me throughout my thesis. I hope they forgive me for inflicting my guitar playing on them more often than was appropriate.

Most importantly, I wish to thank my two fantastic daughters, Kyra and Tara, who have infused my life with so much love. Whatever they do with themselves, they have my support. Similarly, my gorgeous girlfriend, Kris, who is way cooler than she believes herself to be.

Finally, I'd like to thank anyone and everyone who has helped me get to fifty in reasonable shape. Forgive me if you have not received a mention here, but you have my love and respect.

Abstract

This thesis investigates blockchain technology and whether its mutually cooperative topology and commons-based peer production practices have implications for society because, instead of the traditional top-down, centralised model of governance, blockchains represent an alternative way of collaborating.

Much of the literature anticipates the vast potential of the permanent and publicly auditable nature of the propagated values of blockchains. Indeed, writers have supposed that the smart contract capabilities of the technology may prove revolutionary for areas beyond that of the economic domain targeted by the cryptocurrency Bitcoin, which is the first successful use-case of a blockchain. However, few advanced use cases beyond that economic realm have materialised; this research demonstrates such use-cases.

This thesis asks four research questions. The first asks whether blockchains can help reduce energy consumption. The second asks whether blockchains can help digitise the informal sector. The third asks whether blockchains can help counter fake news. The final question asks whether blockchains can help address criticisms of humanitarian aid. Those topics are four amongst many urgent problems currently facing humankind, and therefore, the overarching research question of this thesis becomes whether blockchains can help humanity.

This work advances the supposed potential of blockchains proposed by current literature by using design science research to create software artefacts that propose solutions for incentivising energy efficiency, fighting financial fraud, providing digital provenance and adding trust to humanitarian aid reporting. By demonstrating blockchain-based software solutions in those four topic areas, this thesis concludes that blockchains can help humanity.

However, if they are to help society address some of its problems, blockchains have significant technological and organisational barriers to overcome. Furthermore, the idea that blockchains can help humanity is a form of techno-determinism and this research concludes that it is impossible to solve every issue by diversifying technical operations; humankind must also change political, economic, and cultural goals, too. Nevertheless, this thesis has implications for regulators, despite the barriers and false solutionism offered by technology because, rather than the trusted lawmakers and experts that nations used to look up to as oracles of truth, now it may be possible to look to blockchains, instead.

Publications

Below is a list of works produced by the author during this thesis. Included are software, published papers, an independent media article and invited talks.

Software

The software produced includes a cryptocurrency token and some blockchain-based applications.

Cryptocurrency Token

1. Enervator (EOR). A cryptocurrency that incentivises energy efficiency.

Blockchain Applications

1. Eneradmin (available in the *demo/admin* folder of the Enervator source code repository). Manages the supply of EOR and allows the setting and reading of the token's value parameters.
2. Enerchanger (available in the *demo/exchanger* folder of the Enervator source code repository). Simulates depositing cash and buying EOR.
3. ReportAid. A blockchain-based distributed application (dApp) for humanitarian aid reporting.
4. Provenator. A dApp for proving the origins of digital media.
5. MicroMorpher. An early proof of concept dApp that converts sovereign currencies into Ether (the unit of currency on the Ethereum blockchain).

Published Academic Articles

1. Steve Huckle, Rituparna Bhattacharya, Martin White and Natalia Beloff. Internet of Things, Blockchain and Shared Economy Applications. Procedia Computer Science. Volume 98, 2016, Pages

461-466. September 2016. https://doi.org/10.1016/j.procs.2016.09.074.

2. Steve Huckle and Martin White. Socialism and the Blockchain. Future Internet 2016, 8(4), 49. 18th October 2016. https://doi.org/10.3390/fi8040049.

3. Steve Huckle, Rituparna Bhattacharya and Martin White. Towards a post-cash society: An application to convert fiat money into a cryptocurrency. First Monday. Volume 22, Number 3. 6th March 2017. https://doi.org/10.5210/fm.v22i3.7410.

4. Steve Huckle and Martin White. Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains. Big Data. Volume 5, Issue 4. 1st December 2017. http://doi.org/10.1089/big.2017.0071.

Independent Media

The author published an independent media article during the course of this research.

1. Bitcoin's high energy consumption is a concern – but it may be a price worth paying. The Conversation. 7th November 2018. https://theconversation.com/bitcoins-high-energy-consumption-is-a-concern-but-it-may-be-a-price-worth-paying-106282

Invited Talks

The author was invited to give several blockchain-focused talks during the course of this research.

1. Enervator - Incentivising Energy Efficiency. A talk introducing Enervator, a cryptocurrency that incentivises energy efficiency. 4th October, 2019, as part of 'Innovation forum, Energy Services Business Models', held by the UK Centre for Research into Energy Demand Solutions at The Fusebox, Brighton.

2. Beyond CryptoCurrencies. A talk on some of the software developed during this PhD. 4th June, 2019, at the Brighton Blockchain Meetup in The Walrus.

3. Fake News - a Technological Approach to Proving Provenance Using Blockchains. A talk on fake news and blockchains, as part of the University of Sussex Library's Digital Discovery Week. 9th November, 2018, at the University of Sussex Library's Open Space.

4. Collaborating Through Blockchains. Part of a PhD Symposium at the University of Sussex's Informatics Department. 3rd July 2018, at the Chichester Lecture Theatre at the University of Sussex.

5. Three Minute Thesis - Collaborating Through Blockchains. A three-minute *layperson's overview* of this thesis, given as part of the University of Sussex's Three Minute Thesis (3MT). 27th June 2018, at the Attenborough Centre for the Creative Arts.

6. Introduction to Blockchain Application Development. A three-hour overview of the components of blockchain application development. 19th March, 2018, at Wired Sussex in the Digital Catapult, Brighton.

7. Internet of Things and Blockchain Technology. A twenty-minute overview of blockchains and the Internet of Things. 22nd September 2016, at the Smart Summit London, Kensington Olympia.

8. Internet of Things and Blockchain Technology. An overview of some of the concepts introduced in the author's paper Internet of Things, Blockchain and Shared Economy Applications. 20th September, 2016, at EUSPN 2016, DaMIS Workshop, the International Workshop on Data Mining on IoT Systems at the University of Surrey.

9. Blockchain Technology and the Internet of Things. Overview of blockchains, given at the launch of the Creative Technology Group. 9th May, 2016, at the launch of the Creative Technology Group at the University of Sussex.

10. Evaluating Bitcoin as an Open Source Project. A presentation given to the students on the University of Sussex's Science Policy Research Unit's MSc Module, *ICT Policy and Strategy*. 6th May, 2016, at a University of Sussex seminar on Information and Communication Technology Policy and Strategy.

Table of Contents

List of Figures

Terms

Blockchains. Blockchain is the technology that underpins Bitcoin and Ethereum. Essentially, it is a distributed public ledger of transactions that forms a networked asset database. It includes algorithms that provide a secure mechanism for electronic collaboration without the necessity of garnering trust through a central authority [1].

Commons-based peer production. A mode of production where people work co-operatively to produce goods that are made freely available.

Cryptocurrency. A digital or virtual currency that uses cryptographic authentication [2].

Demonetisation. A process carried out by the Indian Government which withdrew 500 and 1,000 Rupee banknotes from circulation, thereby removing more than eighty per cent of India's physical cash [3].

Fiat money. The noun *fiat* is an authoritative decree, sanction, or order. Therefore, 'fiat money' is currency that is established as legal tender through government regulation [4].

Monetary Sovereignty. The nation-state's ability to exercise exclusive control over its currency.

Smart contracts. Some incarnations of blockchain technology, such as Ethereum, have the ability to execute data-driven application logic, known as smart contracts, which can help automate a system’s rule set [5].

Sovereignty. A phrase meaning *supreme power*. It is an early fourteenth-century word derived from the old French *soverain*. That is derived from the Vulgar Latin superanus, meaning *chief* or *principal*, which itself is a derivation from the Latin *super*, meaning *over* [6].

Acronyms and Abbreviations

API. Application programming interface.
BFT. Byzantine fault tolerance.
BIP. Bitcoin Improvement Proposal.
BTC. Bitcoin.
CBPP. Commons-based peer production.
CPRs. Common-pool resources.
DLS. Dwork, Lynch and Stockmeyer consensus.
DSR. Design Science Research.
EIP. Ethereum Improvement Proposal.
EOR. Enervator - the cryptocurrency created in this thesis.
ERC. Ethereum Request for Comment.
ETH. Ether.
FinTech. Financial Technology.
FLOSS. Free/Libre and Open Source Software.
FLP. Fischer, Lynch and Paterson - FLP impossibility.
GB. The *Grand Bargain* made at the 2016 World Humanitarian Summit.
IATI. International Aid Transparency Initiative.
IETF. Internet Engineering Task Force.
IOT. Internet of Things.
IPCC. Intergovernmental Panel on Climate Change.
LDP. Lean software development.
MVP. Minimum viable products.
P2P. Peer-to-peer.
POS. Proof of Stake consensus.
POW. Proof of Work consensus.
PBFT. Practical Byzantine fault tolerance.
PREMIS. Preservation Metadata: Implementation Strategies.
TPES. Total primary energy supply.
UTXO. Unspent transaction output.
WHS. 2016 World Humanitarian Summit
WMO. World Meteorological Organization.

1 Introduction

This thesis uses design science research to create artefacts that examine whether the in-built mechanisms of blockchains offer solutions to a variety of challenges facing humanity. The problems this work considers are excessive energy consumption, digitising the informal sector, fake news and criticisms of humanitarian aid - a discussion as to why this thesis focuses on those problems, in particular, continues below.

This chapter outlines the background of this work and introduces some related literature. That lays the foundation for describing the research question that is the focus of this dissertation. The chapter then describes the methodology used to examine that research and outlines the thesis' structure. Finally, it shows the contributions to knowledge made, of which there are many, not least applications demonstrating the diverse capabilities of blockchain technology.

1.1 Background

Yochai Benkler, writing at the dawn of the present century, commented:

"An open, free, flat, peer-to-peer network best serves the ability of anyone – individual, small group, or large group – to come together to build our information environment. It is through such open and equal participation that we will best secure both robust democratic discourse and individual expressive freedom" [7]

This thesis examines whether that comment was prescient because it describes the architecture of blockchains, a technology that emerged in 2008, with Satoshi Nakamoto's publication of a white paper that described Bitcoin: A Peer-to-Peer Electronic Cash System [8]. It is the latest instalment of many years of research into blockchain technology in the Informatics Department of the University of Sussex, which began with a collaboration with American Express and an InnovateUK project entitled *Connecting Virtual Communities to the Digital Economy Through Micro-Payment Technologies* [1]. The project's focus was on developing a *design*

fiction [9], shown in Figure 1.1, below. That described an Internet of Things (IoT) prototype called ExpressIT (American Express IoT), which explored the integration of payments into digital economy applications.

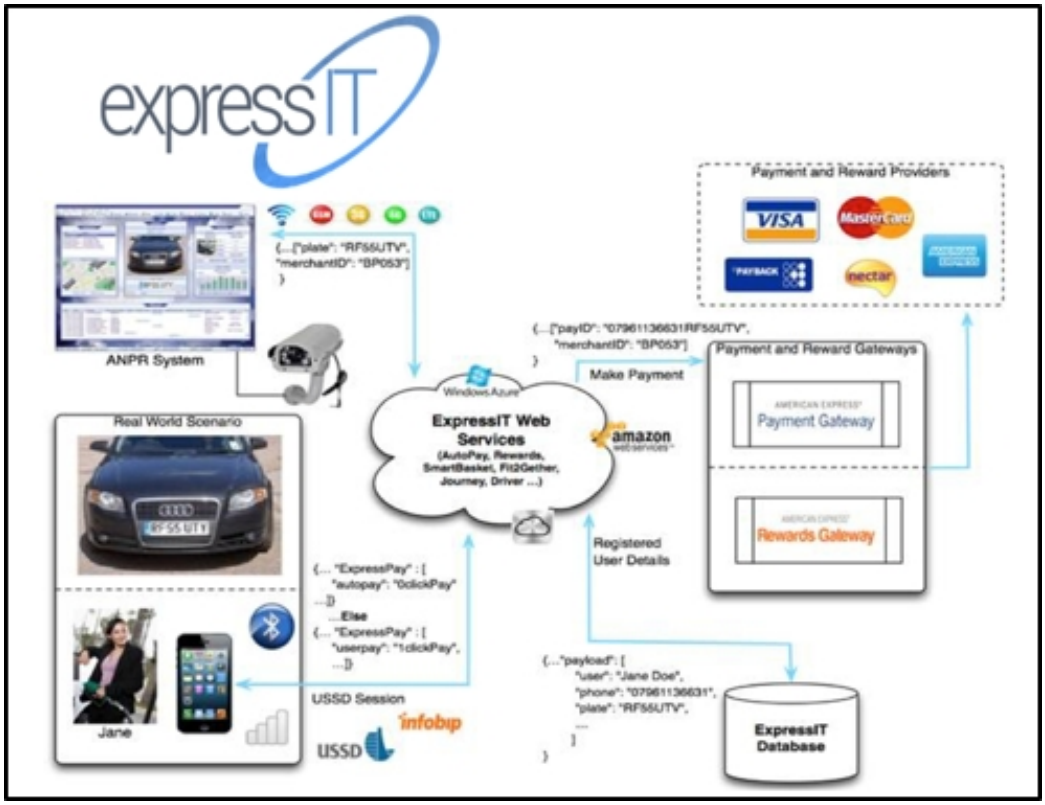


Figure 1.1. The ExpressIT Prototype [1]

The author's paper, *Internet of Things, Blockchain and Shared Economy Applications* [1], continued the work of that InnovateUK project when it began realising the design fictions depicted in Figure 1.1. The article describes everyday social situations for which blockchains are offered as providing solutions because the technology lays the foundations for shared economy distributed applications. One of the paper's scenarios describes an IoT-enabled kiosk that converts foreign cash into its local equivalent. That eventually generated a prototype application called MicroMorpher[1], a tool that converts sovereign currencies into Ether (the native cryptocurrency of Ethereum). The author's paper, *Towards a post-cash society: An application to convert fiat money into a cryptocurrency* [10],

[1]The prototype cryptocurrency exchange application, MicroMorpher, is available on GitHub at https://github.com/glowkeeper/Micromorpher

describes that prototype in detail. MicroMorpher also provides the basis of Enerchanger, an application that is discussed at length in Chapter 7, which converts sovereign currencies into Enervator[2], a cryptocurrency that incentivises energy efficiency. Chapter 6 includes a detailed account of Enervator, the idea for which began in another of the author's papers, *Socialism and the Blockchain* [11], which describes a cryptocurrency token that establishes its value by quantifying the amount of energy used to create that token. Another topic discussed in *Internet of Things, Blockchain and Shared Economy Applications* is digital rights management. That is given further consideration in the author's paper, *Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains* [12], which describes Provenator[3], an application that demonstrates blockchain's potential for proving the provenance of digital media. Chapter 8 discusses Provenator.

This thesis also examines blockchain's suitability for addressing criticisms of humanitarian aid. The idea for that came after an approach made to this author by a Masters student studying with the University of Sussex's Science Policy Research Unit (SPRU), who wanted to explore blockchain's potential in the humanitarian sector. ReportAid[4], a blockchain-based tool for establishing the trust of aid finance reporting, is the result of that initial approach. Chapter 9 describes ReportAid in more detail.

Hence, the basis for most of this thesis is a collaborative InnovateUK project between the University of Sussex and American Express and four published articles of the author. Those have produced several blockchain-based applications, which this thesis describes in detail. Those applications investigate whether blockchains go beyond Nakamoto's original idea for an alternative means of finance [8]. In particular, they allow this thesis to ask if the technology can help address some of the pressing problems facing humanity, namely excessive energy consumption, digitising the informal sector, fake news, and criticisms of humanitarian aid. Those problems, and many more besides, are the result of failures to collaborate in ways

[2]Enervator is open source software, available at https://github.com/glowkeeper/Enervator
[3]Provenator is available at https://github.com/glowkeeper/Provenator
[4]ReportAid is available at https://github.com/glowkeeper/ReportAid

beneficial to everyone and everything, so part of any solution must be improved collaboration. Conway's Law asserts that we design systems that are copies of our communication structures [13]. Hence, if we want mutually collaborative networks, we need networked systems of mutual collaboration. This thesis proposes that Blockchain technology meets that criterion because it is a distributed data store where contributing nodes on the network are peer-to-peer, mutually cooperative and independent of any single controlling entity [11]. A blockchain also has inbuilt cryptographic capabilities, resulting in technology with tools offering confidentiality, integrity, authenticity and validity [12], all of which are properties desirable for the trust necessary in all healthy relationships [14]. The goal of this research is to examine such abilities.

1.2 Related Work

As well as continuing work previously carried out at the University of Sussex via the InnovateUK project, described above, this research also expands the ideas of Swan who promoted blockchains as a technology offering solutions in a wide range of sectors beyond finance [15]. However, this thesis goes further because, whereas Swan describes the *potential* of blockchains, this work demonstrates that potential through applications of the technology.

Rozas et al. examine commons-based peer production (CBPP) and the governance mechanisms of blockchain technologies, which they correlate to Ostrom's principles of sustainable management of common-pool resources (CPR) [16]. Theirs is a world where blockchain technology frames the choices made by society because it becomes an agent of change and helps promote a culture of collaboration [17]. For Rozas et al., such collaboration is due, in part, to the rapid production practices of globally diverse and distributed CBPP development teams; therefore, the governance of CBPP projects often exists outside of any formal organisational structures [18]. Dafermos writes that the Free/Libre and Open Source Software operating system FreeBSD essentially acts as an organisation without authority because the core team do not tell developers what to do; instead, the project proceeds through the direct-

democratic procedures of collective consensus [19]. Rozas et al. believe that blockchains help establish consensus-led governance due to the technology's intrinsic mechanisms of tokenisation, the self-enforcement of formal rules, autonomous automation, decentralisation, transparency and the codification of trust. They argue that such capabilities meet many of the requirements for establishing Ostrom's eight design principles, described below, for the sustainable and equitable management of commons resources [16]:

1. Clearly defined community boundaries
2. Congruence between rules and local conditions
3. Collective-choice arrangements
4. Monitoring
5. Graduated sanctions
6. Conflict resolution mechanisms
7. Local enforcement of regulations
8. Multiple layers of nested enterprises

This thesis examines the claims made by Swan, Rozas et al. and Dafermos when it investigates the governance capabilities of blockchains through practical applications that demonstrate whether the technology's mechanisms may enable it to address a variety of problems. Indeed, the underlying theme of this thesis is governance and how blockchains may be used to organise more fairly. That was a subject first broached in the author's paper, *Socialism and the Blockchain* [11], which considers the social circumstances under which societies may collaborate by using blockchains. The paper proposes that, instead of the usual Libertarian free-market ideals usually associated with the technology, blockchains advocate communitarian modes of governance whereby it could be used to support a Socialist society. For example, *Socialism and the Blockchain* examines the CBPP processes of Bitcoin development, which it correlates to Kropotkin's description of Anarchism, where order emerges through, "an infinite variety of capacities, temperaments and individual energies" [20]. Commons-based peer production is examined in more detail in Chapter 3.

1.3 Research Questions

This thesis has its basis in some of the published work of this author. Amongst many topics of discussion in the author's paper, *Socialism and the Blockchain* [11], was a description of a cryptocurrency token that establishes its value by quantifying the amount of energy used to create that token. That idea provides the basis to Enervator, a cryptocurrency that incentivises energy efficiency. That is described in detail in Chapter 6. Hence, the first research question examined by this work is:

1. Can blockchains help reduce energy consumption?

A scenario depicted in *Internet of Things, Blockchain and Shared Economy Applications* [1], is *John's International Tour*, whereby a businessman, returning home from a trip abroad, uses an Internet of Things-enabled kiosk, coupled to a foreign exchange application on his mobile telephone, to trade his foreign cash for his local currency. The paper concludes that, because the trade uses blockchains, "John knows that he can trust the transaction and that his money is safe". The author's paper, *Towards a post-cash society: An application to convert fiat money into a cryptocurrency*, develops that idea further when introducing MicroMorpher, a prototype blockchain-based application for converting sovereign currency into Ether (the native cryptocurrency of Ethereum) [10]. That paper introduces the Indian Government's process of *demonetisation*, which removed more than eighty per cent of India's physical cash by withdrawing 500 and 1,000 Rupee banknotes from circulation [3]. The move was an attempt to provide banking services to India's unbanked, thereby helping to address concerns over the Indian *informal sector* [21]; a sector that describes the 'unofficial' earning strategies of many of the country's population, which has negative implications for the amount of tax India is able to raise. Demonetisation is described in detail in Chapter 4. *Towards a post-cash society: An application to convert fiat money into a cryptocurrency* asks if the Indian Government could have used MicroMorpher to aid the process. Enerchanger is a progression of MicroMorpher - it is a blockchain-based application for converting sovereign money into EOR and is described in

detail in Chapter 7. This thesis uses Enerchanger to continue the discussion as to whether such a tool might have been used by the Indian Government to help fight tax evasion and financial fraud via blockchain's trust mechanisms [22]. Hence, the second research question examined by this work is:

2. Can blockchains help digitise the informal sector?

Another scenario depicted in *Internet of Things, Blockchain and Shared Economy Applications* [1] discusses blockchains as a tool to help provide rights management of digital audio. That forms the basis to another of the author's papers, *Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains* [12], which presents Provenator, an application that uses blockchains to record and show metadata about the origin, context and history of digital media, thereby helping to prove provenance [23]. Provenator features in Chapter 8 of this work, which continues an examination of blockchain's potential to prove the origins of digital media, and thereby, help fight online propaganda (a topic discussed in more detail in Chapter 4). Hence, the third research question examined by this work is:

3. Can blockchains help counter fake news?

This thesis also examines blockchain's potential for addressing criticisms of humanitarian aid. The plan, initially, was to explore the cryptocurrency capabilities of blockchains as a novel way of providing funds during a humanitarian crisis. However, after some initial research, direct finance via cryptocurrencies was not something this author thought viable at the time. However, the theme of using blockchains for humanitarian purposes still appealed as the author could see the immediate benefit of using blockchains to report on humanitarian aid. ReportAid, a blockchain-based tool for establishing the trust of aid finance reporting, is the result of that idea. A description of that application provides the basis to Chapter 9. Hence, the fourth research question examined by this work is:

4. Can blockchains help address criticisms of humanitarian aid?

The questions described above are four amongst the many problems currently facing humanity. Nevertheless, they are four urgent problems that must be addressed, and therefore, the overarching research question becomes:

Can blockchains help humanity?

The rest of this thesis addresses that overarching problem.

The term *help*, used in each of the research questions above, perhaps requires clarification. Chapter 5 discusses the *principles of implementation* for the applications that form the basis of this thesis, whereby each represents a *minimum viable product* (MVP) (but in a research setting instead of the usual commercial environment). An MVP is, "complete enough to demonstrate the value it brings" [24]; in other words, an MVP *helps* determine the product's potential. Therefore, the term *help* is meant as a substitute for the value demonstrated by each of the applications, whereby they show the potential for blockchains to resolve the problems posed.

1.4 Methodology

The methodological tool used to examine the research objective of this thesis is design science research (DSR), which is a set of analytical techniques for exploring an Information System (IS) [25]. The critical principle of DSR is to achieve understanding by building artefacts that satisfy a set of functional requirements. Figure 1.2 shows the five artefacts created for this work. The first is the unique cryptocurrency EOR, which aims to incentivise energy efficiency. The second is Eneradmin[5], which demonstrates how the various parameters of EOR affect the token's value. The third is Enerchanger[6], which aims to simulate depositing a sovereign currency and exchanging that for EOR, a process that helps frame a discussion around the benefits of using blockchains to digitise the Indian informal sector [21]. The fourth artefact is Provenator, which examines blockchain's potential for proving the provenance of digital media and

[5]Eneradmin is available in the Enervator GitHub repository
[6]Enerchanger is also available in the Enervator GitHub repository

thereby, tackling fake news. The final DSR artefact is ReportAid, which is used to research blockchain's suitability for improving the transparency of humanitarian aid reporting.

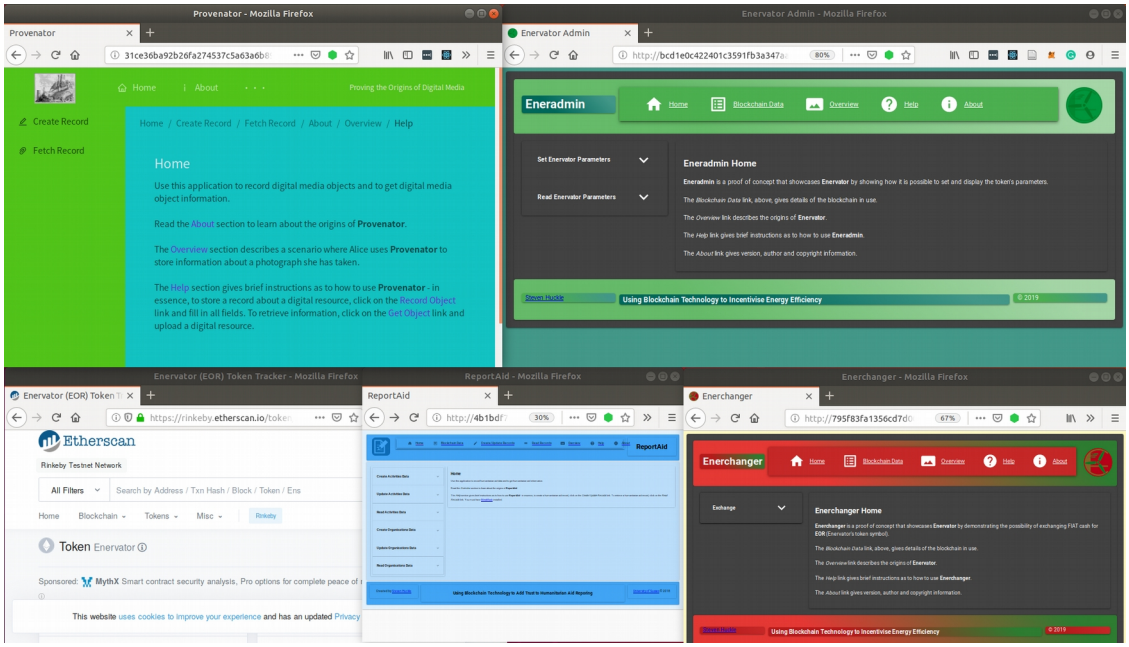


Figure 1.2: The five DSR artefacts described in this thesis. From top to bottom and left to right, 1) Provenator, 2) Eneradmin, 3) EOR, 4) ReportAid, 5) Enerchanger.

1.5 Contributions to Knowledge

The five DSR artefacts created for this work make the following contributions to knowledge:

1. Enervator, Eneradmin and Enerchanger show how it is possible to create a cryptocurrency that incentivises energy efficiency.

2. Chapter 7, which describes Enerchanger, creates a unique scenario by showing how the Indian Government could have used Enervator to help their demonetisation process (described in Chapter 4) and thereby fight financial fraud.

3. Provenator is a unique blockchain implementation of Preservation Metadata: Implementation Strategies (PREMIS), the open standard the application uses to create provenance metadata to verify the authorship and rights of digital media.

4. Chapter 8, which describes Provenator, shows how blockchains could be used to fight fake news.

5. ReportAid is a blockchain-based humanitarian aid reporting application, which is a novel blockchain-based implementation of the International Aid Transparency Initiative (IATI), an open data standard for reporting humanitarian financing. That IATI implementation on the blockchain is also novel.

6. Chapter 9, which describes ReportAid, shows how blockchains could help address criticisms of humanitarian financing.

1.5.1 Published Academic Articles

The basis of this thesis is four published articles, which also contribute to knowledge:

1. Steve Huckle, Rituparna Bhattacharya, Martin White and Natalia Beloff. Internet of Things, Blockchain and Shared Economy Applications. Procedia Computer Science. Volume 98, 2016, Pages 461-466. September 2016. https://doi.org/10.1016/j.procs.2016.09.074

2. Steve Huckle and Martin White. Socialism and the Blockchain. Future Internet 2016, 8(4), 49. 18th October 2016. https://doi.org/10.3390/fi8040049

3. Steve Huckle, Rituparna Bhattacharya and Martin White. Towards a post-cash society: An application to convert fiat money into a cryptocurrency. First Monday. Volume 22, Number 3. 6th March 2017. https://doi.org/10.5210/fm.v22i3.7410

4. Steve Huckle and Martin White. Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains. Big Data. Volume 5, Issue 4. 1st December 2017. http://doi.org/10.1089/big.2017.0071

1.6 Thesis Outline

Chapter 1 is this introduction. It gives an overview of the research that follows.

Chapters 2, 3 and 4, combined, represent a literature review. Chapter 2 introduces some of the research that led to blockchain technology. Chapter 3 examines the politics of blockchains. In particular, it looks at research related to the *commons*, the form of governance this thesis argues enables us to share more equitably. Chapter 4 sets the background for the problems for which this thesis proposes DSR artefacts that can help. In essence, Chapter 4 consolidates the prior technology and politics chapters and explains the gaps in knowledge that this research fills.

Chapter 5 introduces the methodology used to examine the research question; it describes the components of DSR employed in this thesis.

Chapter 6 introduces EOR, a cryptocurrency whose primary goal is to incentivise energy efficiency. That chapter also describes the DSR artefact Eneradmin, the application that administers the parameters that define EOR.

Chapter 7 discusses Enerchanger, the blockchain-based application that converts sovereign currencies into EOR. It creates a scenario where an Indian national exchanges Rupees for EOR, which enables a discussion as to whether blockchains are a useful tool to help digitise the informal sector and, thereby, help fight financial fraud.

Chapter 8 introduces Provenator, the application that attempts to prove the provenance of digital media by recording metadata about that media on the blockchain. That helps frame a discussion about fake news and whether blockchains can counter the phenomenon because they contain the mechanisms for proving ownership.

Chapter 9 demonstrates ReportAid, the DSR artefact for reporting humanitarian financing.

Chapter 10 concludes this thesis by providing answers to the research questions based on the evidence of the DSR artefacts discussed previously. Finally, it introduces the work that could follow this research.

1.7 Summary

This chapter describes the background of this thesis. It is rooted in many years of research into blockchain technology in the Informatics Department of the University of Sussex, which began with an InnovateUK collaboration with American Express. That research has continued with the publication of this author's papers, namely *Internet of Things, Blockchain and Shared Economy Applications* [1], *Towards a post-cash society: An application to convert fiat money into a cryptocurrency* [10], *Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains* [12] and *Socialism and the Blockchain* [11]. Indeed, that last paper proposes that blockchains have the potential to provide the backbone to a Socialist society; in other words, they are capable of organising in a way that is less hierarchical than how much of the Western World currently organises. Indeed, this thesis imagines us cooperating collaboratively rather than competitively, an idea discussed in greater detail in Chapter 3.

Core to this thesis is the research question:

> *Can blockchains help humanity?*

That question is a natural consequence of some of the author's published work, which has generated the following questions:

1. Can blockchains help reduce energy consumption?
2. Can blockchains help digitise the informal sector?
3. Can blockchains help counter fake news?
4. Can blockchains help address criticisms of humanitarian aid?

Chapter 4 discusses those questions in greater detail.

This chapter also introduced DSR, described in detail in Chapter 5, which is the methodological tool used to answer the overarching research objective; that has generated the artefacts that form the core of this thesis and contribute to knowledge. The next three chapters review literature that is pertinent to this work.

2 Blockchain Technology

This thesis researches whether blockchains can help humanity. This chapter gives a technical overview of blockchains, and so it provides the technical basis for this work. Then, Chapter 3 describes the politics of blockchains and blockchain development. That chapter proposes that commons-based peer production is how society might share more fairly. Chapter 4 describes the problems for which this research offers blockchains as a solution; it is where this thesis describes the gaps in knowledge that this research fills. In essence, then, this chapter, Chapter 3 and Chapter 4 form the literature review of this work.

First, this chapter introduces Bitcoin and the Bitcoin blockchain, including a brief history of the technology. Then the chapter describes how distributed systems achieve consensus. Finally, the discussion moves onto Ethereum, which is an implementation of blockchains that can run verifiable applications, a capability used by the design science research (DSR) artefacts that form the bulk of this research.

2.1 Bitcoin

Bitcoin (BTC) came into being as the result of Satoshi Nakamoto's 2008 white paper on a peer-to-peer (P2P) electronic cash system [8]. It is referred to as cryptocurrency because it is a form of electronic currency that relies on cryptographic techniques to prove identity and authenticity and to enforce read and write access to the Bitcoin network.

2.1.1 The Bitcoin Blockchain

BTC was the first successful use case of a blockchain. Figure 2.1 shows the Bitcoin blockchain described in Nakamoto's white paper.

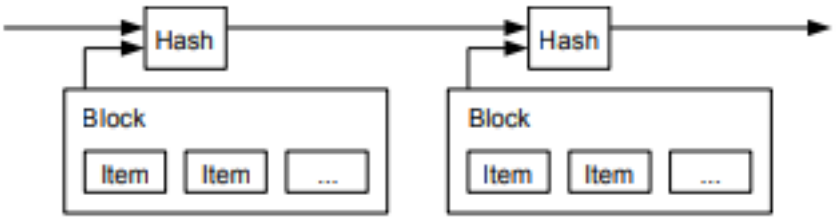


Figure 2.1: The BTC Blockchain [8]

The over-arching purpose of the BTC blockchain is to become a public asset ledger of propagated values, which are coalesced into blocks of transactions, such that a network of multiple sites, geographies or institutions can share, inspect and create new records. The system relies on public-key cryptography to control permissions and track changes; as a result, it is technically infeasible to make changes to values already on the blockchain. Such mechanisms ensure the technology represents a historical record of all transactions ever recorded, so the present state of the blockchain is a deterministic function of the genesis block and that ensuing history [26]. Appendix A gives an overview of some of the cryptographic technologies used by blockchains and consequently, the blockchain-based DSR artefacts described throughout this thesis.

2.1.2 A Brief History of Bitcoin

While there are many examples of successful open-source applications (for example, Linux and the Apache webserver), it is typical for working solutions to appear soon after the conception of the idea. In that respect, BTC is unusual because it is open-source software that is the culmination of work that began in the 1980s, almost half a century ago [27].

In 1982, Chaum and Brand proposed an electronic cash system that would have "a substantial impact on personal privacy as well as on the nature and extent of criminal use of payments" [28]. The 1990 formation of a company called Digicash saw the realisation of that system; unfortunately, it failed to gain much traction, leading to the company folding in 1998. The system had numerous issues because it relied on a single identifiable party, a bank, to sign all transactions. That introduced a single-point-of-failure, as well as giving the signer censorship and double-spending capabilities [29].

Double-spending is where a digital financial transaction is copied and spent in two different places almost simultaneously [11].

The idea of fully digital currencies did not go away. However, whereas Digicash relied upon a central authority, the concept of distributed cryptographic currencies that were not reliant on centralised trust began to gain traction. Wei Dai's b-money [30] and Nick Szabo's Bit Gold contained similar proposals [31]. The latter discusses many principles core to Bitcoin's design, including controlled supply and a Byzantine-fault-tolerant asset registry for storing chained transactions [27]. Byzantine fault tolerance is discussed in detail, later.

In 1997, Adam Back proposed Hashcash, a system initially conceived as a means of limiting unwanted email and preventing denial of service attacks. A 2002 paper saw the system developed further [32], and subsequently, Bitcoin has used the Hashcash algorithm to help prove transactions. Perhaps the first to see the usefulness of Back's ideas was Hal Finney, a developer specialising in cryptography, who used Hashcash to develop his *proof of work* tokens, whereby computing processing was used to guarantee the token's value [33]. The idea of tokenised resources has since reached fruition within Ethereum, an alternative blockchain-based system discussed later. Indeed, this thesis takes advantage of Ethereum's tokenisation capabilities when creating one of its DSR artefacts - Enervator - the cryptocurrency whose aim is to incentivise energy efficiency.

The first reference implementation of BTC was published online in early 2009 [34], and the first transaction of BTC was between Nakamoto and Finney. That took place on 12th January 2009 in block 170, the genesis block, which saw the creation of the system's initial supply of fifty BTC. Below describes Bitcoin in more detail.

2.1.3 Trustless

Nakamoto's white paper raises the problem of legacy electronic cash systems that necessitate trusting many of the third-party financial institutions that had been at the centre of the 2008 financial crisis [8]. For example, supposedly irreversible payments may get reversed, which leads

to expensive dispute mediation, a cost that limits the minimum size of transactions, making very small payments impractical. Moreover, fraud becomes endemic. Bitcoin helps overcome such issues because the system described by Nakamoto is *trustless*, in the sense that it decentralises authority because the network operates without needing to trust any single controlling entity or third-party financial institutions [8]. The discussion below describes how it achieves that. Critical to that discussion is to understand the terms *P2P*, *decentralised*, *distributed* and *consensus*, so those are described next.

2.1.4 Distributed Systems

A *P2P* network is one where participating nodes are both resource providers and resource requesters. Those nodes share the hardware necessary to provide the service and content offered [35]. Furthermore, each node has direct access to other nodes.

The term *decentralised* describes a system comprised of many (possibly geographically diverse), autonomous P2P entities that must seamlessly connect and collaborate. P2P systems do not cede control to one individual or organisation.

This thesis uses the term *distributed* to describe a decentralised system that is logically centralised, whereby it behaves as a single coherent entity. Figure 2.2, below, shows a distributed system that offers each application the same interface, even though it extends over multiple machines.

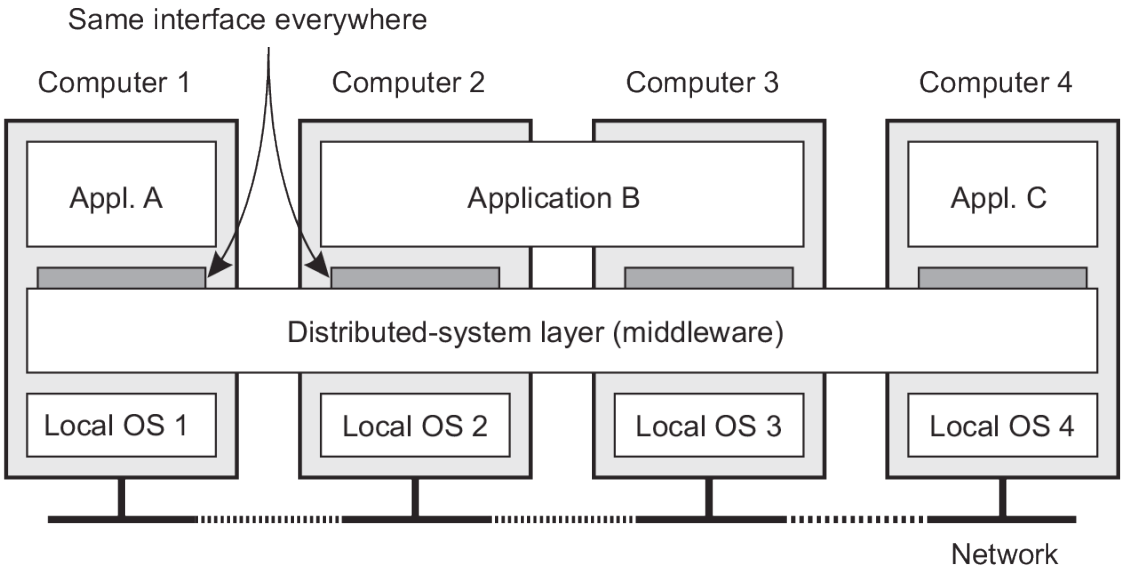


Figure 2.2: A Distributed System [36]

A blockchain is an example of a distributed system because, despite its formation from a collection of geographically independent components, the system with which users communicate is entirely consistent and uniform [36].

Distributed systems have a specific set of characteristics:

1. **Concurrency**. System events occur concurrently, so the order of events needs to be determined.

In 1978, a paper by Leslie Lamport showed that time and order of events are problematic in distributed systems [37]. However, he showed that it is possible to determine whether one event occurred before another by remembering that each node has a sequence of events and messages are sent before they are received. Therefore, by considering separate systems, a partial ordering of events is possible, and a total ordering based on that partiality is possible if each node on the distributed system must hear from the other nodes. However, that total order is reliant on synchronized physical clocks, which are far from trivial to implement.

2. **Message Synchronicity**. Nodes in a networked system communicate and coordinate by passing messages back and forth.

Nodes within a synchronous system have some upper bound of time, T, within which they send and receive messages. Those nodes also have some upper bound of time, P, for the relative difference in speed between nodes.

Synchronous systems are only practical in an idealised setting of a handful of computers in the same room, which have entirely reliable wired links. Even then, nodes can crash or go offline, and messages can be dropped, duplicated, delayed, or received out of order. Hence, some form of asynchronicity is more practical [38]. That is a system that removes both upper bounds T and P so that messages can take arbitrarily long to reach peers, and each node can take an arbitrary amount of time to respond. In essence, that captures the behaviour of the Internet.

A partially synchronous system is a mix of the synchronous and asynchronous models. It is where there exist upper bounds for T and P, but they are unknown beforehand [39].

3. **Failure resistance**. Components in a distributed system may be faulty.

Failures are due to system crashes or malicious attempts at subversion through direct attacks or collusion. Distributed systems should be fault-tolerant [38].

Distributed systems employ various consensus mechanisms to address concurrency, synchronicity and fault tolerance. The discussion below looks at consensus in more detail.

2.1.4.1 Distributed Consensus

Consensus algorithms generally assume three types of actors in a system:

1. **Proposers**. They are often called leaders or coordinators.
2. **Acceptors**. Processes that listen to requests from proposers and respond with values.
3. **Learners**. Other processes that learn the final values [38].

Those actors can achieve consensus if values satisfy the following conditions:

1. **Agreement**. All non-faulty nodes decide on the same output value.
2. **Termination**. All non-faulty nodes *eventually* decide on some output value [38].

In general, the actors follow these three steps:

1. **Elect**. The non-faulty processes elect a Proposer that suggests the next valid output value.
2. **Vote**. Acceptors consider the proposed value, validate it, and if it is valid, vote for it as the next valid value.
3. **Decide**. The non-faulty processes decide on whether that value is the single correct output value. If some criteria of the voting process suggest yes, then the value is validated, and Leaners receive the final value. Otherwise, the whole process begins again [38].

Such consensus steps are almost trivial in a synchronous environment because it is possible to make assumptions about the timing of system events and message delivery. However, in asynchronous distributed environments, no such assumptions can be made. A 1985 paper by Fischer, Lynch, and Paterson (FLP) introduced the idea of FLP impossibility, whereby it is impossible to reach consensus among deterministic asynchronous processes because a single faulty process introduces the prospect of non-termination [40].

The non-termination as a result of FLP impossibility means that consensus is not always possible in a fixed time. One way to circumvent the issue is to use timeouts to make synchrony assumptions [38]. That was the scheme used by the Paxos protocol [41], which became the first real-world, practical, fault-tolerant consensus algorithm:

1. Proposers send a proposal prepare request, n, to a majority of acceptors.
2. Each acceptor promises not to respond to any more proposal prepare requests with values less than n.
3. If a majority of acceptors send responses to the proposers prepare request, then the proposer sends those acceptors a proposal, n, together with a value, v.

4. The acceptors accept the proposal, *n*, only if they have not already responded to a prepare request with a number greater than *n*.
5. Learners find the value, *v*, through a set of distinguished learners, who establish a majority of acceptors has accepted a proposal. Using a broader set of distinguished learners provides better reliability at the cost of increased communication complexity [41].

Paxos adds data to a state log at the rate of one block of information at a time. Although timeouts are not explicit in the algorithm, actual implementations elect a new proposer after some timeout period, a process that results in the termination criteria necessary to overcome FLP impossibility [38]. Implementations of Paxos are assumed safe in asynchronous environments because the algorithm's synchrony assumptions have a known fault tolerance value [42]. However, Paxos is only crash tolerant [38]; it is unable to overcome malicious attempts to undermine a system.

Indeed, it is a challenge to reach an agreement and maintain consistency in a distributed computer system that consists of many computing nodes, any of which could be acting maliciously. It is a conundrum known as the Byzantine Generals Problem because an archaic battlefield analogy describes it succinctly. Loyal generals of the Byzantine army, who are camped with their troops around an enemy city, must reach agreement on a battle strategy. Unfortunately, Figure 2.3, below, shows that one or more of the generals are traitors that attempt to subvert the plan; under those circumstances, how do the loyal generals ensure the Byzantine effort is successful?

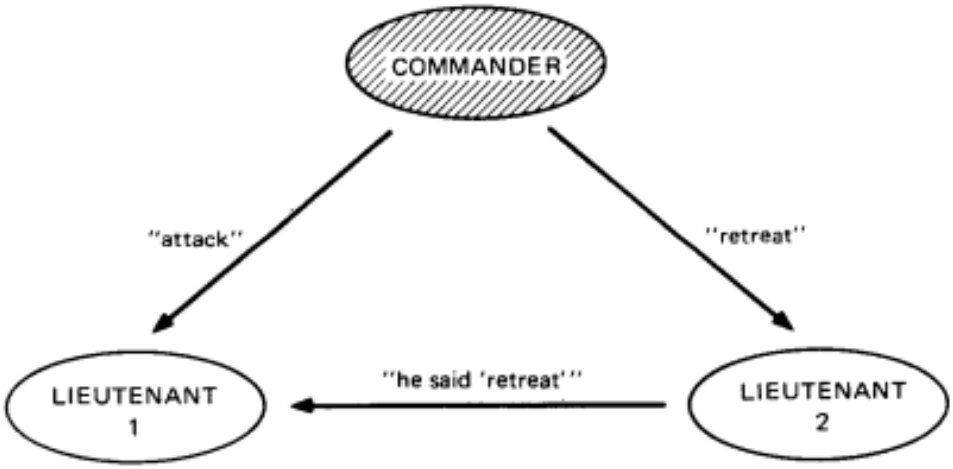


Figure 2.3: The Commander is a Traitor [43]

The solution for distributed computing is to use a Byzantine Fault Tolerant (BFT) consensus protocol that is a global agreement between many, distrusting, anonymous parties [29], such that nodes on a distributed network can decide on a fault-tolerant state of the system. BFT systems must be dependable, even under the circumstances where individual components have failed or where there is imperfect information available. Lamport et al. gave a theoretical solution, via a distributed consensus scheme, in their 1982 paper [43], which shows that the problem is solvable if and only if more than two-thirds of the generals are loyal. However, the paper's BFT solutions are only valid in a synchronous environment, and the search for an asynchronous BFT solution remained elusive. Two algorithms got closer to a solution in that environment.

The first was described in a 1988 paper by Dwork, Lynch and Stockmeyer (DLS), which showed how to achieve BFT consensus in a partially synchronous setting [39]. The paper describes solutions to two assumed partially synchronous systems. The first system assumes that fixed bounds exist for message delivery, but those bounds are unknown beforehand. The second system assumes knowledge of the upper bounds for message delivery, but those bounds are guaranteed only at some unknown *global standardisation Time* (GST). For the former, the goal is to reach consensus

regardless of the actual bounds. For the latter, the goal is to reach consensus regardless of GST.

DLS divides its algorithm into a series of *trying* and *lock-release* phases:

1. A Proposer begins with each of the Acceptors communicating the value they believe is correct.
2. The Proposer *proposes* a value if at least $N - x$ Acceptors have communicated that value.
3. When an Acceptor receives the proposed value from the proposer, it must lock the value and then broadcast that it has locked.
4. If the Proposer receives messages from $x + 1$ Acceptors, showing that they have locked on some value, it commits that as the final value.

DLS constituted a significant breakthrough because it proved that BFT consensus was possible under the assumption of partial synchrony [38]. The paper discusses the safety and liveness properties of distributed systems, which were ideas introduced in 1977 by Leslie Lamport [44]. Safety correlates to the agreement condition of distributed consensus, outlined above, whereby the system assumes that a failure will *not* happen. Liveness correlates to the termination condition. It states that something *must* occur; in practice, it means the system makes progress, no matter what. DLS argued that making a partial synchrony assumption for achieving the liveness condition is enough to overcome FLP impossibility. They proved their algorithms do not need to use any synchrony assumption to achieve the safety condition. They did so by showing that if a consensus algorithm uses timeouts to make some synchrony assumptions, and one of the processes fails, it makes sense for the system to halt. However, where an algorithm guarantees correctness by assuming timeouts, and the synchrony assumption fails, there is a risk that the system forks in two valid directions. Hence, the significant contribution of DLS was to show that a live service is useless if corruption renders it unsafe. In other words, DLS showed that distributed consensus is a trade-off between liveness and safety [38], and that trade-off is possible in partially synchronous settings because some form of timeout is required.

Despite its advances, the DLS notion of time required a form of a clock for synchronicity, which meant it was never fully implemented in the real-world because such clocks are vulnerable to several attacks [38].

A more practical BFT consensus algorithm arrived in 1999 with Castro and Liskov's paper describing Practical Byzantine Fault Tolerance (PBFT) [45]. PBFT was optimised to achieve acceptable response times and did not make any synchrony assumptions for safety since it was safe regardless of how many nodes were faulty [45]. Therefore, it worked in practical asynchronous environments, such as the internet. Below is an overview of the algorithm:

1. Clients broadcast a new value to a Proposer.
2. The Proposer sends the value to all Acceptors.
3. The Acceptors accept the value and send a reply to the Proposer.
4. The Proposer waits for $x + 1$ replies from Acceptors. Once it receives those, the value is final.

However, PBFT did employ a synchrony assumption to guarantee liveness and circumvent FLP impossibility. If more than a third of nodes employing PBFT were faulty, the message delay would grow faster than a specific time limit, and the system would fail. That process works well when the Proposer is non-faulty, but the process for detecting and reselecting a new Proposer becomes inefficient because PBFT needs every distributed node to communicate with every other node on the network. Hence, the algorithm does not scale well and has proved impractical for many use cases [38]. A more practical solution arrived with Nakamoto's BTC implementation [8], described next.

2.1.4.2 Bitcoin Consensus

Nakamoto's BTC implementation was the first computing application to provide production-ready BFT consensus. Indeed, Bitcoin solves many of the scalability issues of PBFT by using overcoming FLP impossibility through using probability, whereby, rather than every node agreeing on a value, nodes agree on the *probability* of correctness [38]. Instead of electing a Proposer to coordinates nodes, BTC uses a P2P network of

distributed transaction validators, who compete to win the right to add transactions to the network by solving a difficult cryptographic problem, a process called 'Proof of Work' (PoW) [46]. Validators, who do not identify themselves to other validators and who are free to enter (or leave) the system at will [29], are figuratively known as *miners* because they are rewarded with Bitcoin when they add transactions to the network, so it is how the system brings new coins into existence. The number of coins given to the successful miner decreases by 50% every 210,000 blocks, or approximately every four years. Such a process occurred in 2016 when the block reward halved from 25 to 12.5 BTC. Such halving means that the number of mined BTC is not expected to exceed 21 million, a maximum reached around 2140 [47]. At that point, miners will be rewarded via transaction fees, which are voluntary payments made on behalf of the processes creating BTC transactions. Thus, miners will retain an incentive to create new blocks [48].

Nakamoto, in his original paper on BTC, describes the algorithmic steps miners must use to create a blockchain network:

1. All nodes receive a broadcast of new transactions.
2. Each node collects new transactions into a block.
3. Each node (miner) tries to find a PoW for its block.
4. When a node finds a PoW, it produces a block that it broadcasts to all nodes. The block contains a timestamp, a difficulty target, and the root hash of a Merkle Tree of all transactions for that block.
5. Nodes accept the block only if all of the transactions it contains are valid. They must not have already been spent.
6. Nodes express their acceptance of the block by working on creating the next block.
7. Nodes use the hash of the accepted block as the previous hash (thus forming the chain) [8].

Individual miners attempt to find a PoW by using an algorithm based on Adam Black's Hashcash [32]. That produces a one-way function, whereby the only way to find a solution is to use brute-force, which amounts to calculating a cryptographic hash of a block's header and a nonce, an

arbitrary number that is used just once so that the hash produced on each calculation is unique. Miners get a list of new transactions that they coalesce into a block. They then send a difficulty target, alongside an 80-byte block header and a nonce, to application-specific integrated circuit (ASIC) hardware optimised to solve the PoW cryptographic puzzle. The ASIC hardware iteratively generates hash values, checking the hash produced against the difficulty target - if the hash is lower than or equal to the target, then the problem is solved. Since the hash must be lower than the target, the calculated value must begin with many zeros. However, the probability of calculating a hash that starts with many zeros is very low; therefore, lots of attempts are required. At each failed attempt, the miners increment the nonce, thus generating a new hash for testing. A golden nonce is one that results in a target hash. Once finding such a value, the ASIC hardware returns the block header to the miner so it can broadcast the block to the network.

However, while it is technically possible for individual miners to mine BTC, the current target difficulty makes that practically impossible and so individual mining farms pool their resources. Pooled miners follow a similar work-flow to solo miners. That allows mining pool operators to pay miners based on their share of the work done. Given that all the miners on the network are performing PoW, the chance of claiming the mining reward is proportional to the fraction of the total computing power of the P2P network [27]. Miners that failed to find a solution get no reward, and as a result, Bitcoin mining has been called 'competitive bookkeeping' [49].

Every 2,016 blocks, the BTC network examines the timestamps of each block header and calculates the time elapsed generating those 2,016 blocks. The ideal value is 1,209,600 seconds, which equates to two weeks, or a single block generated every ten minutes. However, block creation is via a random Poisson process whereby it might be that many blocks, or very few blocks, are found in a given hour [50]. Indeed, if it took less time than two weeks to generate the 2,016 blocks, then the hash difficulty is raised. Conversely, if it took more than two weeks, then the difficulty is dropped [51]. Invariably, as more processing power comes online to the BTC network, the difficulty goes upwards. For example, at the time of

writing, the BTC difficulty is 5,949,437,371,609; since the very first block on BTC had a difficulty of 1, it is now almost 6 trillion times more difficult to mine BTC than it was to mine BTC's genesis block.

PoW relies on a game-theoretic *Nash Equilibrium*, whereby the most profitable operation for each miner is to act in consensus with the majority. That works due to a fundamental concept of BTC - the longest chain. If two versions of the next block on its blockchain are broadcast by different miners simultaneously, the network nodes verify a new block by accepting the earliest transaction. In that circumstance, the system reserves the chain with the later transaction. When the next block is broadcast to the network, if the reserve chain becomes the longest branch, then the network nodes switch to that. In that case, the longest chain has expended the most significant amount of PoW, so as long as the majority of nodes on the network are honest, then the honest chain grows faster than any competing chains. Hence, the majority decision on what constitutes an honest transaction is reached by consensus via the longest chain. Thus, the result is the system stabilises, since no participant gains by changing strategy from that which produces the longest chain [29]. Not all BTC nodes need to store a copy of the whole blockchain. Instead, they only need to keep a copy of the block headers of the longest blockchain and work on the Merkle branch that contains the transaction with the block's timestamp. That assures nodes that it is the right chain because blocks added afterwards act as confirmation that the network has accepted that branch as the longest. Nakamoto called this concept, *Simplified Payment Verification*.

The time stamping and hashing functions of miners help ensure the immutability of the blockchain because block headers are hashes in a chain, and therefore an attacker must change all blocks in that chain to change a single block [52]. That is technically infeasible; the author's paper, Socialism and the blockchain [11] pointed to a study by Harvey, which showed that, in 2014, a computing array with the power of 1,753,694 PetaFLOPS would have been needed to make a fake block on the BTC blockchain [49]. At the time, the world’s fastest supercomputer, the Chinese Tianhe–2, could manage 33.9 PetaFLOPS. That meant that over

50,000 Tianhe–2 supercomputers would have been required to attempt to create a fake block. There are other features built into PoW that help secure the network. For instance, it is unknown which miner will generate a new block, which is an element of unpredictability that makes the system difficult to subvert. PoW relies upon processors, rather than IP addresses, so a malicious actor with the resources to allocate more IPs than anyone else will not benefit. Furthermore, BTC rewards to nodes for creating blocks and verifying transactions gives them incentives to be honest, because it is more profitable for a node to play by the rules than it is to undermine the system [8]. All in all, there is little chance of subverting Bitcoin's safety guarantee. Hence, for practical purposes, Nakamoto Consensus achieves Byzantine fault-tolerance [38].

2.1.4.3 Bitcoin Transactions

Bitcoin's basic unit of account is called a Satoshi, named in homage to the technology's creator. Satoshis represent one hundred millionth, or 0.00000001, of a single Bitcoin. Figure 2.4 shows that the overriding purpose of BTC is the propagation of transactions, which represent owners of Satoshi informing the network that they have transferred ownership elsewhere.

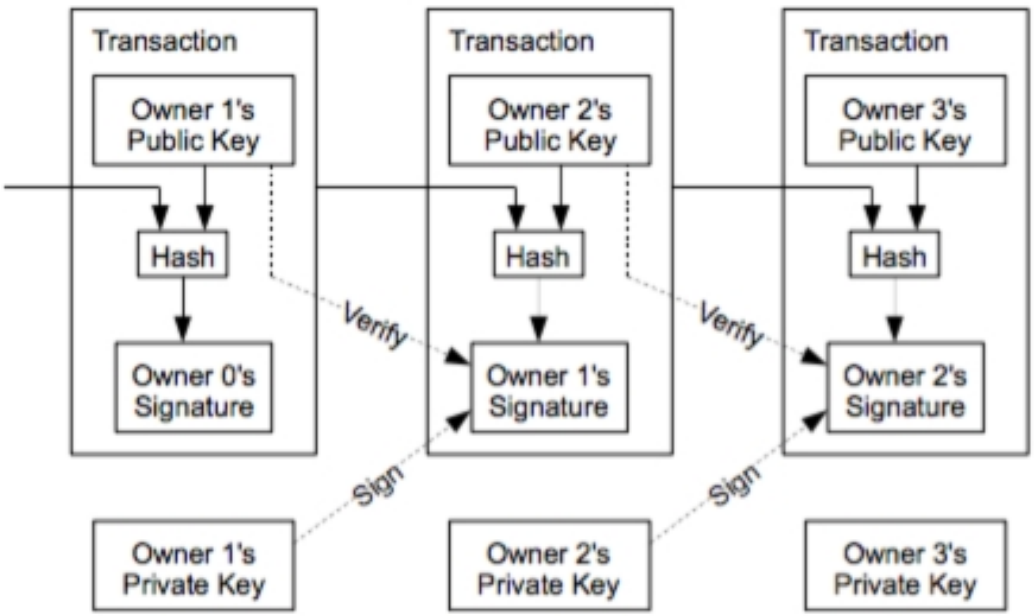


Figure 2.4: BTC transactions [8]

Each BTC transaction has one or many inputs and one or more outputs, whereby each input maps the Satoshi paid to previous outputs, and each new output becomes an unspent transaction output (UTXO). Thus, the system functions as a transaction-based state transition system, which takes a current state, S, a transaction, TX, and if not in error, produces a new state, S' in the form of new UTXO:

```
APPLY(S,TX) -> S' or ERROR
```

Algorithmically, this is:

```
For each input in TX:
   If the referenced UTXO is not in S:
         return ERROR
   else if the cryptographic signature does not match the
   owner of the UTXO:
         return ERROR
   else if the sum of all input UTXO is less than the sum of
   all output UTXO:
         return ERROR
   else:
         remove all input UTXO
         add all output UTXO
   return S'
```

When a BTC address shows a balance of 100 Satoshi, it means that the address has 100 Satoshi in one or more UTXO [53]. That UTXO maps an amount of Satoshi to a transaction output that contains instructions for their ongoing transfer - anyone who wishes to spend those Satoshi must be able to supply the private key that matches the corresponding public key detailed in the UTXO. Those new owners can, in turn, create another transaction that authorises the ongoing transfer. Thus, a chain of ownership is formed [54]. Recording individual transactions on the network would be inefficient, so validators add blocks of transactions, instead. Those blocks contain a timestamp, a nonce, and a hash of the previous block [55]. The network continually updates, producing roughly one block every ten minutes; over time, that creates a persistent, ever-growing, *blockchain* that reflects the latest state of the Bitcoin ledger. The result is a transaction network that behaves similarly to individual lines in a double-entry bookkeeping ledger because they help determine balances within the

BTC network [27]. Hence, the overriding purpose of the BTC network is the propagation of transactions, which exhibit the following qualities:

1. **Authorised**. Transactions are authorised so that only *user x* can perform transactions under the guise of *user x*.
2. **Read-only and Final**. Transactions cannot be modified or deleted.
3. **Uncensored**. A transaction is added to the ledger whenever it conforms to the Bitcoin protocol.
4. **Consistent**. Any transaction added to the ledger conforms to the present state of the system [52].

Public key cryptography ensures authorisation. For Alice to be able to send her Satoshis to Bob, Bob must generate a public and private key pair. To do so, Bob uses Bitcoin's implementation of the Elliptic Curve Digital Signature Algorithm with secp256k1 private keys, which are 256 bits of random data transformed into a secp256k1 public key [53]. Because that transformation is deterministic, the key does not need storing because it is possible to recover it reliably later. Next, the public key is hashed, which is also a repeatable process, so it does not need storing either. Hashing also shortens and obfuscates the key, which gives the system a degree of future-proof security should the supposed one-way property of hashing functions get disproved later. Finally, to produce a valid BTC address and remove the possibility of any ambiguous characters, Bob encodes the hash together with an address version number and an error-detection checksum, using base-58 encoding. He then supplies Alice with his BTC address, which she decodes back to a standard hash that she uses to create a standard Pay-To-Public-Key-Hash transaction output that contains instructions whereby only Bob can spend the Satoshis since he is the only person with the private key corresponding to the hashed public key contained in the output. Finally, Alice broadcasts her transaction to BTC network validators, who, if they deem the transaction as valid, add it as another UTXO.

Coinbase transactions are exceptions to much of the discussion above. They are specialised transactions used for rewarding validators with BTC, so they introduce new coins into the network and, therefore, they are the common origin of a series of transactions [27]. The UTXO of a coinbase

transaction contains a condition preventing its use as an input for at least 100 blocks [53]. That stops BTC validators from spending Satoshis that may get invalidated later.

Transaction consistency happens by encoding transactions into a time-stamped Merkle Tree, shown in Figure 2.5, below, which are efficient binary trees where every leaf node is a data block, and every non-leaf node is a cryptographic hash of its child nodes. Only the root of the Merkle Tree is included in the block's hash and stored in the header. That simplifies immutability to that of the immutability of the block's header [52]. That also ensures efficient storage, since a block with empty transactions is only around 80 bytes.

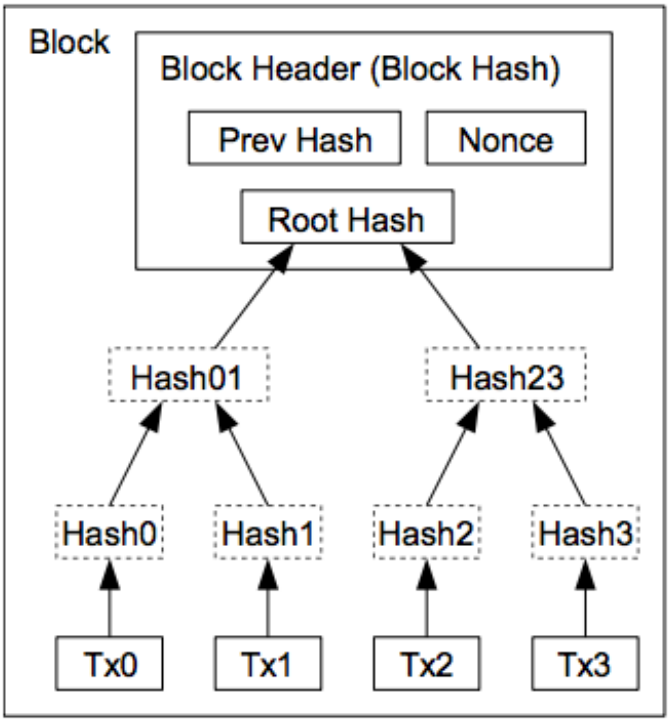


Figure 2.5: The BTC Merkle Tree [8]

The use of Merkle trees allows transactions to be checked against the state of the ledger held in memory, since, "if either (user) A or (user) S has the wrong R (public ledger), they will be unable to complete the protocol with any other legitimate user who has the correct R, a fact that will be quickly detected" [56]. Moreover, as long as a transaction conforms to the protocol's requirements, it is added to the blockchain. Thus, the blockchain

is uncensored. The PoW algorithm requires nodes to perform some form of computational work to establish a trusted identity. That gives BTC a natural way of overcoming 'Sybil Attacks' [57], which are where a single malicious entity can present multiple identities, enabling it to gain control of a system for nefarious purposes [58]. PoW also solves the problem of double-spending in a distributed environment, so recipients can trust that someone else hasn't already spent their coins.

2.1.5 The Bitcoin Blockchain as a Database

Greenspan describes the Bitcoin blockchain as a distributed multi-version concurrency control (MVCC) database, "with a few more bells and whistles" [59]; in essence, blockchains solve the multi-master replication problem of distributed systems [52]. At first glance, the comparison to a database appears valid. First, the current set of unspent BTC transaction outputs (UTXO) form the whole database, whereby each UTXO is a single row in a table. Secondly, one or more of those outputs creates one or more new outputs, which is much like a database transaction that deletes one or more rows and then creates one or more new rows. Thirdly, blockchains include mechanisms that ensure a single output cannot be spent by more than one transaction, much like MVCC databases guard against the deletion of a single row by more than one transaction. Fourthly, the total quantity of units in the inputs to a transaction must cover the total quantity of units in the outputs, a rule that disallows transactions from increasing the number of units on the network. That is similar to a database stored procedure, except that it is impossible to circumvent.

Perhaps, then, the comparison between a blockchain and a distributed database is merely superficial. Indeed, the BTC blockchain has capabilities far beyond traditional distributed databases because it includes exchange mechanisms that allow for the secure and seamless transfer of assets, which it achieves without relying upon any form of centralisation [15]. Furthermore, blockchains use public-key cryptography to create UTXOs, which means, unlike any database, they include a publicly auditable UTXO permission scheme.

2.2 Ethereum

BTC is an open-source GitHub project[7], and so any developer can fork the code and create their implementation of its underlying blockchain technology. Indeed, since its launch in 2009, Bitcoin has spawned a group of alternative blockchains. They have popularly became known as *altcoins* [60]; some of the more well-known examples are Litecoin, Ripple and Stellar. Perhaps the best known, however, is Ethereum, a system first proposed in a white paper by Vitalik Buterin [55]. Ethereum is a blockchain technology that has capabilities above and beyond BTC because the platform uses a decentralised virtual environment, the Ethereum Virtual Machine (EVM), to provide a Turing-complete operating system that offers the ability to create distributed applications. The network went live on 30th July 2015.

2.2.1 Consensus

At the time of writing, Ethereum uses a PoW consensus scheme for for checking the validity of a block of transactions, similar to Bitcoin. Its white paper gives an algorithmic description of the process [55]:

```
If the previous block exists and is valid:
   If the timestamp of the block is greater than that of the
   previous block:
        If the timestamp is less than 2 hours in the future:
             If the PoW on the block is valid:
                  S' = APPLY(S,TX)
                  If ERROR:
                       return ERROR
                  else:
                       return S'
```

Whereas BTC has a block confirmation time in the order of ten minutes, at the time of writing, Ethereum achieves a block confirmation time of approximately fifteen-seventeen seconds. However, faster block confirmation introduces issues of 'orphaned blocks', known as uncles, which are old blocks that do not make it onto the main Ethereum blockchain. It achieves that by taking advantage of the protocol 'Greedy

[7]Bitcoin's source code is available at https://github.com/bitcoin/bitcoin

Heaviest Observed Subtree' (GHOST) [61]. The problem is as follows: if node A mines a block and then node B mines another block before A's block propagates to B, B's block might not get validated and, therefore, it becomes orphaned because it does not form part of the chain. Furthermore, suppose A is a mining pool with one-third of the processing power of the entire network, and B has one-tenth of that power. Under such conditions, A's risk of producing orphans is two-thirds, whereas B's risk is nine-tenths. Hence, a short block interval that produces a high stale rate has the result of ensuring that A's size makes it considerably more efficient. Thus, large mining pools may gain control of the network [61]. The original GHOST protocol, proposed by Yonatan Sompolinsky and Aviv Zohar in December 2013 [62], solved the problem of fast confirmation times by using uncles in its calculation of the longest chain. Ethereum goes further by giving block rewards to miners that created stale blocks dating back seven generations [61].

2.2.2 Ether

The cryptocurrency used to transfer value within the Ethereum network is called *Ether*. The smallest denomination of Ether is the Wei, where Ether describes a unit that is one quintillion (10^18) Wei.

2.2.3 Gas

Ether is the reward Ethereum mining nodes receive for the services they provide. However, Gas, rather than Ether, is used to calculate the amount of work done when miners execute operations on the EVM; by maintaining a unit independent of Ether, the Ethereum network can, in theory, stabilise transaction costs.

The concept of Gas includes the following terms:

1. **Gas Cost**. A static value that describes the computation costs relative to Gas. The value is stable and never changes.
2. **Gas Price**. The cost of Gas relative to Ether. The Gas Price varies to keep the same real value.
3. **Gas Limit**. The maximum amount of Gas, per block.

4. **Gas Fee**. The reward that miners receive [63].

The idea is that users pay for the transactions they submit. They offer a Gas Price for each unit of Gas, up to and including a Gas Limit, which is the maximum amount of Gas a user is willing to spend. There is also a minimum - 21000 Gas, which is the cost of transferring Ether from one external account to another (accounts are discussed below). Hence, the Gas Fee is equal to the *Gas Cost x Gas Price*, which is converted to Ether and paid to the miners. Consequently, the higher the Gas Price the user sets, the more likely they are to get their transaction mined faster since miners will prefer transactions with the highest reward.

2.2.4 Ethereum State Machine

Similar to BTC, Ethereum is a state transition system. However, instead of UTXO, the Ethereum state is comprised of objects called *accounts*, whereby state transitions are direct transfers of value between those accounts [55]. The system features externally owned accounts and contract accounts. External accounts are controlled by private keys and have no associated application code. They create and sign transactions that are sent either to other external accounts or to contract accounts. Contract accounts are controlled by the code they contain; hence, Ethereum refers to contract accounts as *smart contracts*, because they can run blockchain addressable scripts that represent verifiable application logic [11]. When contract accounts receive transactions, they activate their associated code, whereby they can read and write to the blockchain and send other messages to other contracts. Smart contracts are discussed in more detail, below.

2.2.5 Smart Contracts

The phrase 'smart contract' was first coined in 1994 by Nick Szabo [64]. Szabo considered a smart contract as an electronic transaction protocol that did not require trusted intermediaries for executing contractual arrangements, such as payments. Back then, Szabo considered some Point of Sale systems as having implemented limited smart contract functionality. Today, Ethereum's smart contracts represent promises to

provide some predefined functionality, an ability of which the DSR artefacts that form the core of this thesis take advantage.

In reality, most Ethereum smart contracts are not exceptionally smart! Those underpinning DSR artefacts described later in this thesis are a case in point since, aside from some elementary arithmetic and a tiny amount of logic, mostly they represent simple *set* and *get* operations. That is because of the idea of *gas*, introduced above, whereby users are charged to perform computations on the blockchain, so less code leads to less expensive execution. Also, the *gas limit* imposes a maximum cost to those computations, and any function exceeding that maximum fails. Given those conditions, it makes sense to keep smart contracts as simple as possible, which means moving as much application complexity as possible away from the blockchain.

Appendix B details the costs of deploying the smart contracts used by the DSR artefacts described in this work.

2.3 Summary

This chapter lays the technological foundations for much of the rest of this work because it describes blockchains. It first gives some background to the cryptocurrency that was the first successful incarnation of a blockchain - BTC, including a brief historical overview of BTC, distributed systems and distributed consensus. That enabled a description of the BTC proof of work consensus algorithm. Bitcoin is central to much of the current interest in blockchain technology, enabled, in part, because it is based on the open-source principle of commons-based peer production (described in Chapter 3). Hence, other technologies, known as *altcoins* have built on Bitcoin's success by forking its code-base, and Ethereum is an example of that. It began by using Bitcoin's PoW consensus algorithm and added the EVM, capable of executing Turing-complete programs, known as *smart contracts*, a capability used by the DSR artefacts that are central to this research.

3 The Politics of Blockchains

This thesis researches whether blockchains can help humanity. The previous chapter, Chapter 2, described the technological capabilities of blockchains and laid the basis of this work. This chapter describes the political and social context of those capabilities and proposes that commons-based peer production is how society might share more fairly. The next chapter, Chapter 4, describes the problems for which this research offers blockchains as a solution. In essence, then, Chapter 4 is where this thesis describes the gaps in knowledge that this research fills. Together, Chapter 2, this chapter and Chapter 4 form the literature review of this work.

First, this chapter discusses the predominant right-wing political view of Bitcoin (BTC) and suggests that, by contrast, the capabilities of blockchains encompass a left-wing, Socialist philosophy. Indeed, blockchain technology is the result of the *commons* and commons-based peer production (CBPP), which is a socially egalitarian mode of governance that is distinct from the predominant economic mode of production of the Western world [65].

3.1 Right versus Left

BTC is considered a Libertarian ideological vehicle [66]. However, this author's paper, *Socialism and the Blockchain* [11], argues that the technology underpinning BTC, the blockchain, has properties that make it an ideal tool for supporting Socialist societies.

3.1.1 Libertarianism and Cryptocurrencies

Libertarianism advocates a raft of personal freedoms, such as freedom of speech, freedom of worship, legal equality, the right to bear arms, moral autonomy and the right to private property. Hence, Libertarians hold a deep scepticism of collective action, the state and government power [67]. They lobby against a monetary sovereign, suggest the scrapping of fiat money and promote disbanding centralised banking systems because they entail risks that are, ultimately, underwritten by the people [68]. Indeed,

Libertarians oppose government monetary issuance policies that control the value of cash because they support the freedom of individuals to decide on the subjective value of anything they wish to use as a means of exchange [11].

Hence, to a U.S. Libertarian, cryptocurrencies, such as Bitcoin (BTC), hold an enormous political potential; indeed, Bitcoin technology has many properties that mean it has become associated with the ideology of extreme Libertarian individualism [11]. The Literature Review describes many of those properties; they include Bitcoin's algorithmic management of money supply, which, as has been explained above, holds the prospect of subverting government money sovereignty and the monetary policy capabilities of central banks [69]. There is no single authority in control of cryptocurrencies because a distributed P2P network verifies transactions, not centralised clearinghouses. BTC miners, rather than governments, receive *seigniorage* (which is the revenue earned by issuing the currency. Seigniorage occurs in several ways, but the most important is the profit made due to differences between production and distribution costs and the value of money itself [70]). BTC also promotes privacy because the cryptographic capabilities inherent in the technology make it challenging to match transactions to real people [66]. Furthermore, BTC can be traded or exchanged without needing to trust any centralised financial institution [71], a factor that would have helped individuals circumvent much of the contagion of the financial crisis of 2008. Indeed, Yermack notes the 'interesting' timing of BTC's release, coming as it did at the time of the depths of that crisis [72].

3.1.2 Socialism and Blockchains

As opposed to the Libertarian ideal of extreme individuality, the various forms of Socialist philosophy (such as Marxism, Utopian Socialism and Anarchism), share many egalitarian commonalities, not least their wish for flat (non-hierarchical) societies [20]. Socialists also promote various forms of social ownership involving communitarian means of production and distribution [73]. Hence, blockchain technology has features ideally suited to Socialist ideology because Nakamoto's non-hierarchical design, where a

community of validators providing cooperative consensus [8], result in a technology that has native support for distributed, communitarian peer-to-peer networks. Below discusses peer-to-peer collaboration in more detail.

3.2 Commons-Based Peer Production

The author's paper, *Internet of Things, Blockchain and Shared Economy Applications* [1], set the scene for much of this thesis since it created scenarios that showed how blockchain's decentralised applications might allow people to operate in a shared digital economy. The article's overriding theme was enabling people to "monetise their things", whereby it proposed there will be many opportunities to profit financially in such an economy. This section looks at a different way in which blockchains allow people to profit, not necessarily financially, but in terms of personal development. It describes commons-based peer production (CBPP), which is where producers become consumers [74], and where goods are made freely available. Hence, the design artefacts featured in this thesis, which are all open source and freely available on GitHub, are products of CBPP.

3.2.1 Fully Rational Individuals

During her prize lecture, after receiving the 2009 Nobel Prize for Economics, Eleanor Ostrom describes the dominant economic view of the mid-twentieth century Western world [65], which she explains is where all human activity revolves around economic competition. That reduces everything - time, property, production, the creations of people, people themselves — to the status of objects at the disposal of Capitalist profit margins [75]. Price becomes the primary means of measuring the need and utility of scarce resources, and the only means by which a fair price is reached is through the creation of price-based markets. In other words, competitive markets enable the discernment of value [76]. Those markets rely on a division of private and public, whereby the market becomes the primary means for the production and exchange of private goods. For public goods, only the state can impose the rules and regulations that make people refrain from self-interested activities [65]. Private goods are exclusive and rivalrous because people are excluded from ownership unless

they pay for them, and once someone obtains those goods, no one else can own them. By contrast, public goods are non-excludable and non-rivalrous, because no one can own them, and individual use does not prevent use by others. Game theory underpins much of that because, given a ruleset governing social interaction, humankind can reason and optimise the outcome [77]. Thus, the dichotomy of market versus state relies on *fully rational individuals*, who, given all possible information regarding strategies and the favourability of different outcomes given those strategies, make reasonable decisions.

3.2.2 Common-Pool Resources

Ostrom argues that a complete theory based on rational individuals is insufficient. That is because it cannot explain all of human social existence. For example, it fails to cover the many ways people organise, because, "what is called 'rational choice theory' is not a broad theory of human behaviour but rather a useful model to predict behaviour in a particular situation – a highly competitive market for private goods" [65]. Hence, Ostrom attempts to fill the void by adding two additional categories to public and private goods - toll goods and common-pool resources (CPRs). A private golf club is an example of a toll good. It differs from private goods because it enables non-rivalrous but small-scale exclusive use of its golf course. Whereas, the U.K.'s forests are an example of CPRs. They differ from public goods because they are non-exclusive but rivalrous since, to share the forests' resources fairly, they need managing. Hence, Ostrom's CPRs form a part of the commons, "things that no one owns and are shared by everyone" [78].

Castells believes that models of governance similar to Ostrom's CPRs are gaining traction and that Western democracies are witnessing a shift away from hierarchical constitutions, towards a networked society that is decentralised and peer-to-peer [79]. That is a move that some consider as crucial to our development [80].

3.2.3 The Tragedy of the Commons

However, not everyone is confident as to the success of such a move, citing 'the market' as "cruel and relentless", whose participants "destroy the commons because they dislike the competition" [78]. Moreover, recent history has derided the commons model; in a famous paper, *Tragedy of the Commons*, Hardin denounces the commons as open to exploitation [81]. He creates a metaphor for the problem of overpopulation by describing a situation where a herdsman with cattle on an open pasture considers the utility of adding more animals to his herd. Hardin argues that the herdsmen are the sole beneficiary of the profits got from that added cattle, but everyone else shares the loss of pasture. Hence, he has much to gain by adding animals, and little to lose, so he adds more and more to his herd. However, other herdsmen reason the same and also add more, which leads to overgrazing and, eventually, to the collapse of the pasture. In other words, Hardin's tragedy is that "freedom in a commons brings ruin to all" [81]. A similar situation would occur if a greedy woodcutter felled too many trees in the forests described above.

3.2.4 Managing the Commons

However, academics have since refuted Hardin's argument, "the commons were not really common, there was no tragedy" [82]. That is because Hardin depicted an un-managed pasture, which had no boundaries, no management and no rules. His was an exposition of the prisoner's dilemma, a classic exposition from non-cooperative game theory, where all players have all the information regarding strategies and outcomes, but they are unable to communicate. That leads to a state where, if the non-communicating prisoners make their optimum choices, "individual rational strategies lead to collectively irrational outcomes" [83]. Ostrom argues that it is infeasible to develop a formal game for analysing more complex social settings [65]. Unlike the prisoners' dilemma, communication is the foundation of commons models, which have boundaries, rules, social norms and sanctions for exploitation [78]. For example, the forestry CPRs, detailed above, are *managed*. They feature *polycentric management*, a form of distributed governance where the decision making process for each

forest is decentralised and independent, resulting in consistent regulation that functions coherently and exhibits predictable patterns of interdependence [65].

Hardin's *tragedy* is easily refuted empirically by merely studying successful commons. Indeed, an examination of ancient commons models may help us reconnect with established traditions [80]. Long before the modern industrial age, systems based on mutuality appear to have thrived in all the unenclosed lands of the world. Peoples as diverse as the Irish Clachan, the long-fallow agricultural North American tribes, the semi-nomadic Aboriginals [84] and the hunter-gatherers of African villages practised such methods [85]. Whereas hunter-gatherer societies are often portrayed (by modern economists) as backward, there is growing evidence that they were, in fact, affluent. That is because their aim was not to maximise market utility (price); instead, it was to satisfy all the material wants of their communities. In that endeavour, they profited greatly [86], because they managed to meet the needs of their communities sustainably. If endurance is the measure of a particular civilisation's success, then the African bushmen are by far the most successful, stable and sustainable civilisation in human history; after all, recent studies suggest they flourished for well over 150,000 years [87].

Notwithstanding the success of the mutually cooperative systems of the African hunter-gather societies, a specific English agrarian practice is the best-known example of a commons [85]. The 6th November 2017 marked the 800th anniversary of the 1217 Charter of the Forests [88], which established the commons as rights of access to the royal forests to commoners so that they could use them for food, fuel and pasture [88]. The Charter of the Forests is complementary to the Magna Carta, *the Great Charter*, which was decreed at Runnymede, near Windsor, in the U.K., on 15th June 1215. Initially drafted by the Archbishop of Canterbury, the Magna Carta was an attempt to build peace between King John of England and a group of rebel barons. Unfortunately, that first version of the charter was a failure, but a 1225 redraft was successful, and the Magna Carta became law [89]. Some of the provisions made then still stand (one example is that the English church shall be free), making the Magna Carta

the longest standing English legal enactment. However, various parliamentary enclosure acts eroded the rights established by the Charter of Forests [90]. Its last rights were repealed in 1971 [89].

3.2.5 The Digital Revolution

However, the ideals of the commons appear to be flourishing in this age of the Digital Revolution [91], which is the dawn of an information society that has prospered since the latter half of the twentieth century [92]. It is the latest of a series of revolutionary developments driving human progress through the late modern era (from the mid-eighteenth century onwards). That period has witnessed the Industrial Revolution (1770–1850), an age founded upon the discovery of water-based mechanisation processes. The age of steam-powered thermodynamics followed (1850-1895). Then the age of electrification (1895-1940). Next was the age of motorisation, enabled through mechanical and chemical engineering (1940-1970) [92].

The Internet is perhaps the most significant innovation of the Digital Revolution. In its early days, it was predominantly the playground of Computer Scientists and University Scholars. Then, in the 1990s, the establishment of the World Wide Web (WWW) made the Internet available to the broader public [93]. Indeed, the twenty-first century has seen the Digital Revolution continue apace; in the period 2000-2017, Internet usage increased tenfold, and by then, over half the world's population used it regularly [94]. The Internet would not exist (as we know it today) without the philosophy of 'free and open', via free/libre and open-source software (FLOSS). For example, the protocol suite TCP/IP, which is the foundation of most of the communication that happens on the network, is governed by the Internet Engineering Task Force (IETF), an open standards committee. HTTP is part of the TCP/IP protocol suite, which forms a core part of how the World Wide Web operates. Historically, much of the content of the WWW has been served by the Apache Web Server [95], itself an open-source product. Indeed, much of the digital age's software has been placed in the public domain and made available for free. That is because, in the early part of computing history, software was not thought to have the same copyright status as literary works.

In 1974, the U.S. Commission on New Technological Uses of Copyrighted Works changed that, when they decided that "computer programs, to the extent that they embody an author's original creation, are a proper subject matter of copyright" [96]. Ten years later (and perhaps as a reaction against the growing commercialisation of software), the free software movement began, with the creation of the GNU Project [97]. That laid the framework for the development of the operating system Linux, perhaps the best known free software project, which Linus Torvalds first announced in 1991 on the comp.os.minix Usenet group. The Open Source Initiative (OSI) was created in 1998. OSI has gone on to establish the qualities required for open source development, namely, free redistribution of the code (including its source), non-discriminatory behaviour, and non-restrictive licenses [98]. Technologies founded on such principles, coupled with the proliferation of online social spaces have created a self-reinforcing loop, or 'viral spiral' [99], making many new products freely available. Hence, free software represents a way of organising that creates *digital commons* [74].

3.2.6 Digital Commons

The digital commons movement creates a space inhabited by *digital commoners*, which is a self-determining, politically independent collective of ethnically and geographically diverse voluntary communities of artists, lawyers, scholars, technologists and activists [100]. They are attempting to make society much more participatory [101]; after all, the relationship between the organisation of society, its values and its social processes is significant [102]. In so doing, they are instituting a type of a digital rhizome [103] that encompasses the values and norms that inform the creative processes for managing the interdependence between resources, community and a set of standard protocols [104]. Within the movement, producers also become consumers [74] because users are free to run, study, modify and redistribute software [105]. Thus, the digital commons employs a cooperative model, which, rather than through the dominant hegemony of hierarchical corporate structures, creates goods using practices from CBPP [106]. Hence, the movement is an expression of Ostrom's principles and a new, non-market and cooperative mode of

production that is a cultural shift away from the industrial economy and production that is inherently centralised, monopolised and hierarchical [74].

3.2.7 The Wealth of Networks

CBPP provides a counterweight that transforms Adam Smith's The Wealth of Nations into The Wealth of Networks [107]. The practice expands on the classical economists' simplified dichotomy between Capitalism and Socialism, or market and state, thereby offering an alternative from either private market-based property regimes and public ownership [108]. That counterweight is due, in part, to the characteristics of digital goods, which are naturally abundant because they can be copied, shared and modified ad infinitum [74]. Therefore, to enable market exchange, Capitalist regimes make digital goods artificially scarce. That is because, under marketised systems, the insufficiency of material is the starting point of all economic activity [86]. That creates an immediate barrier to uptake because someone must go without if they do not have the means of purchase. Instead, CBPP produces value by sharing resources freely; the movement believes in the freedom to know rather than the freedom to own [109], whereby anyone can obtain, test and extract the software's value, a process that allows innovation to flourish [110]. In short, by removing the price hurdle and making goods freely available, CBPP creates assets that, as opposed to Capitalism, are much more socially egalitarian.

There are many examples of successful CBPP technologies, including the free encyclopedia Wikipedia[8], the FLOSS operating system FreeBSD[9], and the FLOSS website content management system, Drupal[10]. Another example is Bitcoin, which introduced the world to blockchains, which has native support for peer-to-peer collaboration within a distributed communitarian network [111]. Indeed, Rozas et al. describe the correlation between blockchains and the commons governance principles of Ostrom, and proposes that, rather than promoting a culture of competition, the

[8]Wikipedia is available at https://www.wikipedia.org/
[9]FreeBSD is available at https://www.freebsd.org
[10]Drupal is available at https://www.drupal.org/

system suggests a culture of cooperation [16]. The technology's cooperative model is also highlighted by Wright et al., who advocate for blockchain technology becoming the enabling solution for collective social institutions [112]. Furthermore, Scott writes that Anarchist traditions depend upon small-scale egalitarian structures created through the interdependence of societal members, to which blockchain systems may be directly applicable because the technology provides methods of governance that allow autonomous collaboration [113].

3.3 Summary

This chapter sets the political context for the rest of this thesis. First, it recognised that BTC is primarily considered as a Libertarian ideological vehicle [66]. However, this author's paper, *Socialism and the Blockchain* [11], argues that the technology underpinning BTC, the blockchain, has properties that make it an ideal tool for supporting Socialist societies. The idea was that such societies feature less inequality than many of the countries in the Western World. That is because Nakamoto's non-hierarchical design, where a community of validators provide cooperative consensus [8], results in a technology that has native support for distributed, communitarian peer-to-peer networks. Much of the rest of the chapter focused on peer-to-peer collaboration and, in particular, FLOSS and commons-based peer production, a mode of governance that this chapter proposes is how a networked society might collaborate more fairly. Indeed, the DSR artefacts that feature in this thesis are themselves FLOSS applications, and they were built using FLOSS tools.

4 Benefiting Humanity Through Blockchains

This thesis researches whether blockchains can help humanity. That research is examined through the lens of four subordinate questions:

1. Can blockchains help reduce energy consumption?
2. Can blockchains help digitise the informal sector?
3. Can blockchains help counter fake news?
4. Can blockchains help address criticisms of humanitarian aid?

This chapter sets the background to those questions, and by so doing, it explains the gaps in knowledge that this research fills. It completes a literature review that began with the previous two chapters; Chapter 2 outlines the technological capabilities of blockchains, and Chapter 3 discusses the political and social context of those capabilities.

First, this chapter describes some of the work that has inspired this thesis, which proposes blockchains have the potential to go beyond finance. Then, it describes the problems that the research questions address, and for which the design science research (DSR) artefacts, which are the focus of this thesis, are proposed as solutions.

4.1 Cryptocurrencies and Beyond

This thesis has its basis in some of the published work of this author. The author's paper, *Internet of Things, Blockchain and Shared Economy Applications* [1], creates three scenarios that describe the ability of blockchains to enable people to operate securely in a shared economy. The third of those scenarios relates to digital rights management; in other words, it is a use of blockchains beyond economics. Indeed, in her 2015 book about the promise of blockchain technology, Swan writes that the irrevocable, publicly auditable transactions of blockchain technology could usher in an era that revolutionises not just the economy, but also political, humanitarian, social and scientific domains. In other words, blockchains could "reconfigure all aspects of society and its operations" [15].

Swan defined such potential as Blockchain 1.0, 2.0 and 3.0, where 1.0 represents cryptocurrencies, 2.0 represents financial applications, and 3.0 represents applications beyond finance. This thesis follows a similar progression when describing the DSR artefacts in this thesis. Chapter 6 describes a blockchain 1.0 cryptocurrency, Enervator (EOR), which aims to incentivise energy efficiency. Chapter 7 features a blockchain 2.0 financial application, Enerchanger, a DSR artefact that demonstrates converting sovereign currencies into EOR. Chapters 8 and 9 discuss blockchain 3.0 applications beyond finance. Chapter 8 focuses on Provenator, which is a DSR artefact that examines blockchain's potential for proving the provenance of digital media. Chapter 9 describes ReportAid, a blockchain-based tool for establishing the trust of humanitarian aid reporting. Therefore, in contrast to Swan, who talks about the *potential* of blockchains, this thesis *realises* that potential through innovative, practical applications of the technology.

4.2 Blockchains and Energy Consumption

The author's paper *Socialism and the Blockchain* included a discussion about the amount of energy consumed by the Bitcoin (BTC) network [11]. The paper estimated that BTC used as much as the total consumption of the people of Jamaica. In an article for The Conversation[11], *Bitcoin's high energy consumption is a concern – but it may be a price worth paying* [114], this author concluded that Bitcoin's commons-based peer production (CBPP) practices (CBPP is discussed in Chapter 3), were a rebuttal to the consumption-led ideology of Neoliberalism [114]. The piece argued that, by providing an alternative, BTC might indirectly drive down the energy use of society. However, the author was left wondering if he could produce a more immediate response to those criticisms. Enervator, a cryptocurrency that incentivises energy efficiency, which is the topic of discussion in Chapter 6, is that response. It is a DSR artefact that allows this thesis to examine the first research question:

Can blockchains help reduce energy consumption?

[11]The Conversation - https://theconversation.com - is a not-for-profit organisation. They source topical content, written by academics, that is written in plain English and aimed at the general public.

Below puts energy consumption in context.

4.2.1 The Climate Emergency

Climate change is a disturbing reality that raises the spectre of extinction [115]. Growing public awareness of the issue may lead to the conclusion that global warming is a relatively modern discovery. However, science has suspected the excesses of the Industrial Revolution may be catastrophically changing the earth's atmosphere for over one hundred and fifty years. In 1859, John Tyndall found that hydrocarbons block the radiation in different gases, and in 1864, he proposed that changes in atmospheric concentrations of carbon dioxide might affect long-term weather patterns. In 1896, Nobel Laureate Svante Arrhenius predicted that burning coal would warm the planet, a prediction tested and promoted in the 1930s by steam engineer Guy Callendar [116]. By the late 1950s, science had become increasingly insistent that carbon emissions could have drastic effects on the earth's climate [117]. In 1965, U.S. President Lyndon B. Johnson's Science Advisory Committee warned of the harmful effects of fossil fuel emissions [118]. Around the same time as President Johnson's report, Murray Bookchin wrote an article in which he bemoans humanity's global despoliation of the environment. He wrote that was disrupting the atmosphere, climate, water resources, soil, flora, fauna and all the necessary cycles of nature, which he claimed were disasters threatening the stability of the earth's ecosystem [119]. Bookchin prescribed much of that destruction to the burning of fossil fuels that create a blanket of carbon dioxide, stopping heat escaping the earth's atmosphere, leading to the planet's temperature rising. He predicted, correctly, that such processes eventually lead to more violent storms, a melting of the polar ice caps and rising sea levels that inundate vast tracts of land.

4.2.2 The Greenhouse Effect

In 1972, John Sawyer published a study that accurately predicted the "Greenhouse Effect" and the rate of global warming caused by hydrocarbons [120]. That same year saw the Club of Rome report, "Limits to Growth", which mentions anthropogenic increases in carbon dioxide and

associated effects on the climate [121]. In 1979, the World Meteorological Organization (WMO) convened the World Climate Conference, which declared, "an increased amount of carbon dioxide in the atmosphere can contribute to a gradual warming" [122]. In 1988, the WMO and the United Nations Environment Programme formed the Intergovernmental Panel on Climate Change (IPCC), a body tasked with providing the world with an authoritative and objective technical assessment of scientific evidence on anthropogenic effects on the earth's atmosphere. In a 2006 report for the U.K. Government, Nicholas Stern, chair of the Grantham Research Institute on Climate Change and the Environment at the London School of Economics, looked at the effects of global warming on the world economy. There, he remarked, "Climate change is the greatest market failure the world has ever seen" [123]. The review warned that a continuation of the prevalent economic growth model of Capitalist societies, or business as usual (BAU), would increase the risks of severe, irreversible impacts on the essential elements of life for people around the world. Stern predicted that it would be the poorest who suffer the most [123]. The IPCC's Fifth Assessment Report (AR5), published in 2014, says human influence on the climate system continued to grow, to the extent that all the world's ecosystems showed signs of severe adverse impact [115]. AR5 makes four climate projections, which are dependant on different pathways for carbon emissions. They range from a scenario where the world undertakes stringent mitigation (RPC2.6), through two intermediate scenarios (RPC4.5 and RPC6.0) and one extremely alarming scenario (RPC8.5), where BAU allows emissions to keep growing. According to AR5, the cumulative annual temperature increases under RPC8.5 risk pervasive and irreversible damage, including wide-spread impacts on unique ecosystems, thereby threatening food security, compromising normal human activities and causing the extinction of many species.

The Paris Agreement, signed in 2016, called on nations around the world to undertake ambitious efforts to combat climate change [124]. The agreement aims to strengthen the global response to the threat of environmental collapse by keeping global temperature rises well below two degrees Celsius above pre-industrial levels. It also promises additional help

for developing countries to adapt to the worst effects of climate change. Unfortunately, on June 2017, U.S. President Donald Trump announced that the U.S. would cease all participation in the Paris Agreement, alleging it undermines the U.S. economy. During a news bulletin on BBC Radio 4 on Monday 4th December 2017, a reporter summarised a meeting of the United Nations Environment Assembly (UNEA), in Kenya, where measures to cut pollution met stiff resistance, "as governments balance health and environmental concerns against economic growth" [125]. The latest evidence shows such moves to be incredibly short-sighted. The WMO produces an annual statement regarding the state of the climate; its latest report lists 2015–2018 as the four warmest years on record [126]. The ocean is warmer than it has ever been, and global mean sea levels are rising. Arctic and Antarctic sea-ice extent is falling well below average. The result of all that is extreme weather, which has impacted on lives on every continent.

4.2.3 People Are Demanding Action

Given the climate crisis, people around the world are demanding action. Extinction Rebellion is an international movement that uses non-violent civil disobedience to try to achieve radical change to minimise the risk of human extinction and ecological collapse[12]. They are calling for governments around the world to act immediately to help halt biodiversity loss and reduce greenhouse gas emissions to net-zero by 2025. Greta Thunberg is a Swedish schoolgirl who has become famous for initiating a youth movement that strikes for action on climate change[13]. On 1st March 2019, one-hundred and fifty students from the global coordination group of the youth-led climate strike, including Thunberg, issued an open letter to the UK's Guardian newspaper:

"We, the young, are deeply concerned about our future. Humanity is currently causing the sixth mass extinction of species and the global climate system is at the brink of a catastrophic crisis. Its devastating

[12]You can read more about Extinction Rebellion at https://rebellion.earth/

[13]Information about The school strike for climate action is available at https://www.schoolstrike4climate.com/

impacts are already felt by millions of people around the globe. Yet we are far from reaching the goals of the Paris agreement.

Young people make up more than half of the global population. Our generation grew up with the climate crisis and we will have to deal with it for the rest of our lives. Despite that fact, most of us are not included in the local and global decision-making process. We are the voiceless future of humanity.

We will no longer accept this injustice. We demand justice for all past, current and future victims of the climate crisis, and so we are rising up. Thousands of us have taken to the streets in the past weeks all around the world. Now we will make our voices heard. On 15th March, we will protest on every continent.

We finally need to treat the climate crisis as a crisis. It is the biggest threat in human history and we will not accept the world's decision-makers' inaction that threatens our entire civilisation. We will not accept a life in fear and devastation. We have the right to live our dreams and hopes. Climate change is already happening. People did die, are dying and will die because of it, but we can and will stop this madness.

We, the young, have started to move. We are going to change the fate of humanity, whether you like it or not. United we will rise until we see climate justice. We demand the world's decision-makers take responsibility and solve this crisis.

You have failed us in the past. If you continue failing us in the future, we, the young people, will make change happen by ourselves. The youth of this world has started to move and we will not rest again." [127]

Thus, the world's youth are calling for governments to address the crisis. On 15th March 2019, an estimated 1.4 million students, from one-hundred and twelve countries, joined Thunberg in striking and demanding climate action [128]. What form should that action take? Bookchin's prescient 1964 article might offer some clues [119]. In that, he describes the science of ecology, which harmonises nature and humanity and, in turn, releases the power of a diversified society, driven by the humanity of the spontaneous

individual who is unencumbered by a state-lead authority. Bookchin argues that freeing people from the shackles of authority unleashes their creativity, "we would see a colourful differentiation of human groups and ecosystems, each developing its unique potentialities and exposing members of the community to a wide spectrum of economic, cultural, and behavioural stimuli. Falling within our purview would be an exciting, often dramatic, variety of communal forms" [119]. He argues for human-centred forms of production, which would allow humanity to become as creative as it was during the Renaissance, a time when old institutions were swept aside, thus unearthing real potential through the creation of entire sciences and philosophies. That would free human imagination and help overcome the problems caused by centralisation and bureaucracy and any forms of domination. Thus, such a society would be anchored by decentralised popular assemblies that dispense with the injustices of Capitalism and the endless crisis caused by exploitative Capitalist markets [129]. Bookchin calls that *Communalism*, which is a system where technology becomes a critical enabler that, to reveal its humanism, is assimilated and given an organic perspective [119]. He argues that none of that assimilation is possible without rebalancing the earth's ecosystems and re-introducing more variety to sources of energy, through renewable technologies, such as wind, solar and wave. As well as diversity, contemporary commentators discuss increasing the resilience of communities by improving energy efficiency and reducing demand. However, the challenges there are immense, not least because, at the global level, there is a strong correlation between increased wealth and increased energy consumption [130].

The DSR artefact Enervator employs blockchains, the technology that assimilates the decentralised architecture that characterises many of Bookchin's ideas. Enervator offers an economic incentive for decreasing energy demand, and this thesis examines whether that may help address the concern over the correlation between increasing wealth and increasing consumption. Chapter 6 examines Enervator in more detail.

4.3 Blockchains and Digitising the Informal Sector

The author's paper *Internet of Things, Blockchain and Shared Economy Applications* includes a scenario called *John's International Tour*, whereby a businessman, returning home from a trip abroad, uses an Internet of Things-enabled kiosk, coupled to a foreign exchange application on his mobile telephone, to trade his foreign cash for his local currency [1]. The paper concludes that "John knows that he can trust the transaction and that his money is safe", because the trade uses blockchains. The author's paper, *Towards a post-cash society: An application to convert fiat money into a cryptocurrency*, develops that idea further when introducing MicroMorpher, a prototype blockchain application for converting sovereign currency into Ether (the native cryptocurrency of Ethereum) [10]. That paper discusses the Indian Government's attempts to provide banking services to India's unbanked, many of whom use 'unofficial' earning strategies via India's *informal sector* [21], which has negative impacts on the amount of tax the country is able to claim [10]. *Towards a post-cash society: An application to convert fiat money into a cryptocurrency* asks if the Indian Government could have used MicroMorpher to aid the process. Enerchanger, described in Chapter 7, is a blockchain-based application for converting sovereign money into EOR that is a progression of MicroMorpher. Indeed, this thesis uses Enerchanger to continue the discussion as to whether such a tool might have been used by the Indian Government to help fight tax evasion and financial fraud via blockchain's trust mechanisms [22]. Hence, Enerchanger is a DSR artefact that allows this thesis to examine the second research question:

> *Can blockchains help digitise the informal sector?*

Below describes the problems of the informal sector.

4.3.1 The Informal Sector

The World Bank defines the informal sector as that which leads to 'unofficial' earning strategies [21]. That covers both criminal activities as

well as casual and temporary jobs, paid for in physical cash, thus enabling tax evasion. A 2014 study estimated that the Indian informal sector amounts to some forty per cent of their economy, and as a result, the government received up to two-thirds less tax than it might have done [131]. Indeed, a 2016 report by the Global Innovation Exchange estimated that the use of physical cash costs India up to US$3.5 billion annually [132]. Whereas the global average was sixty-two per cent, in 2014, just fifty-three per cent of the adult Indian population held a bank account [133]. Furthermore, forty-three per cent of those accounts were inactive. The result was that just eleven per cent of the Indian public used a debit card in 2015 and cash accounted for ninety-seven per cent of Indian retail transactions [132].

4.3.2 Demonetisation

The Indian Government's demonetisation process, which began in late 2016 through the withdrawal of 500 and 1,000 Rupee banknotes, removed more than eighty per cent of India's physical cash [3]. The move was the latest of a range of legislation announced for digitising the Indian informal sector. A September 2016 report by McKinsey gave those measures further justification; it predicts that, by 2025, global efforts to digitise the informal sector will boost the economy by up to US$3.7 trillion [134]. Among India's measures include their September 2010 announcement of Aadhaar, a national identity scheme for all Indian residents involving a 12-digit unique number, linked to biometric data, such as photographs, fingerprints and iris scans [135]. 2011 saw the launch of RuPay (a portmanteau of the words Rupee and payment), a payment card scheme accepted at all Indian ATMs which offers an alternative to MasterCard and Visa [136]. Then, in early 2014, the Royal Bank of India (RBI), the central bank to whom the Indian government have deferred money issuance rights, announced the removal from circulation of all pre-2005 banknotes [137]. The summer of 2014 saw the Prime Minister of India, Mr Modi, announce *Pradhan Mantri Jan Dhan Yojana*, which translates to *Prime Minister's People Money Scheme*. The aim was to give the Indian population universal access to mobile banking facilities by allowing them to open a bank account without a deposit [138].

In July 2015, Mr Modi also announced *Digital India* [139], a scheme to help improve internet infrastructure, online government services, and computer literacy. The Unified Payments Interface launched in April 2016 [140], which is where a single mobile application system unifies the online payment infrastructure of participating Indian banks. 2016 also saw an initiative to replace debit and credit cards with Aadhaar-enabled payments [141].

The effect of demonetisation was dramatic. Immediately, there was a significant spike in bank deposits [142], a tenfold increase in digital transactions [143] and a near threefold year-on-year increase in collected taxes [144]. Additionally, by 2016, measures such as Pradhan Mantri Jan Dhan Yojana resulted in India becoming the second-largest smartphone market in the world, with 220 million users [145]. As of January 2019, India also ranked second in the world for the number of active Internet users, with 560 million [146].

However, India's 560 million active Internet users represent just 41.8 per cent of the population, so there remains plenty of scope for improving the country's digital infrastructure. This thesis proposes a potential innovative solution to digitisation via Enerchanger, a DRS artefact that converts sovereign currency into Enervator. Chapter 7 discusses that proposal more thoroughly.

4.4 Blockchains and Digital Provenance

One of the scenarios depicted in the author's paper, *Internet of Things, Blockchain and Shared Economy Applications* [1], discusses blockchains as a tool to help provide rights management of digital audio. That forms the basis to another of the author's papers, *Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains* [12], which presents Provenator, an application that uses blockchains to record and show metadata about the origin, context and history of digital media, thereby helping to prove provenance [23]. Provenator features in Chapter 8 of this work, which continues an examination of blockchain's potential to prove the origins of digital media, and thereby, help fight online

propaganda, a topic discussed in more detail below. Hence, Provenator is a DSR artefact that allows this thesis to examine the third research question:

Can blockchains help counter fake news?

Below puts fake news in context.

4.4.1 A History of Fake News

It appears that misinformation, in the form of propaganda, is particularly prevalent in this age of the Digital Revolution [12]. However, material that has been distorted or decontextualised to deceive has been around since time immemorial. For example, the earliest example of propaganda is considered to be the 515 BC Behistun Inscription on a cliff at Mount Behistun in Kermanshah Province, Western Iran. That documents the rise to the throne of the Persian Empire of Darius I. It claims his right to rule by extolling his royal virtues and glorifying his early military campaigns [147].

4.4.2 The Origins of Propaganda

In 1622, Pope Gregory XV formed the 'Congregatio de Propaganda Fide', the Congregation for the Propagation of the Faith, for disseminating and transmitting Catholicism throughout the world (the institution still exists today, although it has been renamed the Congregation for the Evangelisation of Peoples). Indeed, the etymological roots of 'propaganda' are from the Latin 'propagare', which means propagation. Thus, propaganda is often understood to mean the proliferation of some form of ideology.

Many regard Edward Bernays' 1928 publication as the manual of propaganda [148]. Bernays documents the steps necessary for engineering public opinion through the distortion of the facts; its somewhat sinister opening paragraph argues that it is imperative that democracies deliberately manipulate the habits of society because such invisible manipulation constitutes the dominant ruling power [12]. However, the book must be put in context because it was not long before its publication that the word propaganda had taken on its pejorative sense.

4.4.3 War Propaganda

During the First World War, stories began to materialise of the deception that was used by the political machinery of the Allied forces to demonise *The Hun*. An example of such falsification was the misinformation directed by Conservative MP John Charteris, Head of Intelligence for the British Government. He transposed headlines from a story about a train carrying dead horses onto another lamenting a German train of fallen infantry who had died on European battlefields. Charteris used his fabrication to falsely accuse the German military of fuelling their war effort by extracting glycerine from dead soldiers, a lie that was intended to persuade China onto the Allied side. That proved unsuccessful and worse consequences followed; the Nazi Party used such propaganda as evidence of the deception of the British, which commentators suggest led to people doubting news of actual atrocities by the Germans during the Second World War [149].

However, even before the onset of that war, the Nazi Party formed the Reich Ministry of Public Enlightenment and Propaganda; despite using evidence of British falsification against their enemy, they realised the importance of conveying an ideology by manipulative deception through the control of media [12]. Indeed, heading that ministry was Joseph Goebbels, who commented, "If you tell the same lie enough times, people will believe it; and the bigger the lie, the better" [150]. Stalinist Russia also used propaganda techniques. During the 1930s, Soviet media began censoring dissonant voices and would frequently claim that its citizens' living standards were higher than those of the Capitalist West [151]. That misdirection continued after the war, too, when State newspapers propagated an idealised fantasy far removed from the reality for ordinary Russians [152]. Russian television, radio and cinema gave credence to such falsehoods [12], by depicting, triumphantly, the happy, fulfilled lives of a fictional public, who were supposedly living the 'Soviet dream' [152]. The U.S. Government were equally guilty of post-war media control. To counter the Soviet propaganda effort, they instigated policy NSC/10, which detailed wide-ranging covert propaganda operations [153]. Such manipulation

continued throughout the 1960s and 70s when U.S. media organisations promoted the benefits of Western lifestyles, a move similar to that undertaken by Soviet state media. Such practice was intended to exert financial pressure on developing nations, thus undermining their attempts at self-determination and promoting Western business interests [154].

4.4.4 Modern Uses of Propaganda

Even after Glasnost in the 1990s, which contained policies aimed at opening up political and social discussion, Russian propaganda has continued. Sergei Shoigu, the Russian Minister of Defence, admitted that, in 2013, his government established an organisation called 'Voyska Informatsionnykh Operatsiy', whose aim was the smart propagation of misinformation [155]. Russian State media produced a photograph they claimed showed the passenger aircraft MH17 being shot down by an unknown jet fighter and not, as Western governments claimed, by Russian-backed Ukranian Separatists during their annexation of Crimea. The authenticity of that photograph has since been called into question by an anti-propaganda agency called StopFake, who cite various irregularities as proof that the picture is fake [156].

On June 4th, 1989, up to one million people joined a student demonstration in Beijing's Tiananmen Square. The students were calling for greater democracy, freedom of the press, and freedom of speech [157]. Figure 4.1, below, shows an iconic image from the protest; it symbolises the Chinese people's defiance of state oppression and their opposition to the Chinese government's violent crackdown of the demonstration, whereby many of the protesters were injured or killed. However, while that picture would be recognised internationally, it is not quite so well known within China. That is because, in the thirty years since the protest's violent suppression, the Chinese authorities have been busy censoring all reporting of Tiananmen. The result is that they have successfully managed to erase the demonstration from the Chinese public's collective memory. It is an act of propaganda designed to legitimise China's current leadership and its narrative of the past, the present and the future, whereby the Chinese

Communist party is promoted as the driver behind a "harmonious society" [158].

Figure 4.1: Tiananmen Square Protest

Western governments remain involved in propaganda, too. For example, in 2005, the U.S. Government spent US$300 million on manipulating news stories that attempted to cast a favourable light on the Iraq War [159]. In a recent interview, Janis Sartis, the Director of a NATO Strategic Communications Centre, said, "You don't need tanks. You might actually achieve your goals if you change the perception of a given society in a way that corresponds to your interests and the society starts to act how you want them to act" [160].

4.4.5 Social Media Propaganda

The author's paper, *Fake News: A Technological Approach to Proving the Origins of Content* [12], recalls George Orwell's Nineteen Eighty-Four, which depicts state oppression through historical revisionism via the (successful) censorship and modification of media, such as photographs [161]. Indeed, the job of the book's central character, Winston Smith, is to distort facts by rewriting newspaper articles in a manner that corresponds

to the state's propaganda. By casting a negative light on the actions of a tyrannical government, Orwell demonstrates that press freedom is at the core of a healthy society [12]. Indeed, a free press is supposed to be a central tenet of many of the nations who opposed both Fascism in the Second World War and Soviet Communism during the Cold War [12]. For example, the First Amendment to the U.S. Constitution guarantees individual and press freedom. It prohibits government from Orwellian interference on those freedoms, "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances" [162].

The free press of Western democracies is under pressure from various sources. For example, a recent U.K. survey showed that public trust in traditional news sources has fallen very low. That might be due, in part, to President Trump, who frequently attempts to discredit stories with which he disagrees, by claiming, "fake news!" [163]. Unfortunately, it is often challenging to spot invented propaganda and fake news from those that are real [12]. For example, when the U.K.'s Channel 4 News showed three false and three real stories to nearly two thousand adults, only four per cent were able to identify all the articles correctly, and nearly half thought that at least one of the fakes was real [164].

The sources of where people get such news are changing quickly, due to the growing influence of online media and social networks. Nowadays, it is impossible to understand the effects of propaganda without accounting for social media [165]. Platforms such as Facebook, Twitter and Instagram may also amplify 'homophily', which is the tendency of people to make associations with those who represent some form of similarity. Thus, there is the danger such platforms constitute a loud and polarising form of 'echo chamber', which foster agreement in some viewpoint, thereby strangling debate because woe betides anyone holding a contrary opinion. That is not good for democracy because such restricted worlds result in citizens who only accept information that fits their particular outlook [166]. Online systems also feature algorithms that amplify misinformation so that it

quickly scales to the millions of users on those platforms. Such algorithms do not prioritise factual information, but rather, they prioritise engaging content, which may or may not be accurate. Trending algorithms go viral, and virality suggests consensus [167].

The result is that social media exacerbates the problem of fake stories. For example, there is now no question that Russia interfered with the 2016 U.S. Presidential election by spreading falsehoods through social media [167]. There has been analysis that shows that stories about the U.S. presidential election garnered much less interest via traditional news outlets than they did on Facebook [168]. That fact is recognised by the company itself, who admitted that people use their platform to debate elections and promote ideology [169]. Hence, politicians have realised that social media companies play an essential role in deciding the outcome of elections [170], so those companies have come under political pressure to counter the problem of falsehoods and political propaganda. Indeed, commentators have called for regulatory and oversight frameworks to ensure the accountability of private tech' platforms [167]. In response, social media companies have announced numerous initiatives, including third-party verification of news items, regularly giving users tips on how to spot false stories and interface redesign that makes it more convenient for the public to report those falsehoods. Additionally, the origins of political advertisements on such platforms have become more transparent [171].

4.4.6 Fake News Detection Using Artificial Intelligence

In evidence given to the U.S. Congress, Facebook Chief Executive, Mark Zuckerberg, said that the company was researching the use of artificial intelligence (AI) systems for detecting fake stories. However, he was not sure how long it would be before AI alone would be able to spot such stories reliably [172].

Meanwhile, information science is attempting to use automated methods for verifying online information [173]. City University has instigated a

Google-sponsored research and development project called DMINR[14], which aims to help journalists check news stories. The DMINR Artifical Intelligence (AI) system attempts to merge information retrieval and deep learning technologies to gather news and analyse the underlying trends. While still in development, the intention is to create a human-centred AI platform that is sympathetic to the skills of traditional journalism [174]. Recent research suggests the City team have a challenge ahead of them. For example, researchers from MIT, Qatar Computing Research Institute (QCRI) and Sofia University in Bulgaria used an extensive dataset to train a news' classifier that calculated the trustworthiness of media outlets. During tests, that correctly characterised the news items just sixty-five per cent of the time; while better than a coin flip, the result suggests there is still some way to go before AI can reliably detect social media stories intended to mislead. Among the biggest challenge is the sheer volume of data, which is often incomplete, unstructured, and contains lots of additional 'noise' in the form of auxiliary information [175]. That differs from the analysis of traditional big data, which features highly structured networked information, where patterns are discernable [176].

Although the MIT study shows that AI has some way to go before it can detect fake news reliably, Facebook has successfully used AI to help identify counterfeit media by verifying the system's recommendations through human review. In September 2018, a photo circulated on Brazilian social media that claimed to show Senator Gleisi Hoffmann standing next to the man responsible for the stabbing of the-then Presidential candidate Jair Bolsonaro. Facebook's AI systems identified the possibility that the image was false, and a team at the Brazilian fact-checking organisation Aos Fatos confirmed that falsehood by showing that the image was not elsewhere from Juiz de Fora, the scene of the stabbing [177]. Hence, it appears that, currently, AI fake detection is merely a complement to human effort. This thesis examines a similar approach when proposing the DSR artefact Provenator, a tool that allows content creators to establish the provenance of the digital media they create. That is discussed in more detail in Chapter 8.

[14]See more about DMINR at https://blogs.city.ac.uk/dminr

4.5 Blockchains and Humanitarian Aid Reporting

This thesis examines blockchain's potential for addressing criticisms of humanitarian aid. ReportAid is a blockchain-based tool for establishing the trust of aid finance reporting; hence, it is a DSR artefact that allows this thesis to examine the fourth research question:

> *Can blockchains help address criticisms of humanitarian aid?*

A description of ReportAid provides the basis to Chapter 9. Below puts the criticisms of humanitarian aid in context.

4.5.1 Criticisms of Humanitarian Aid

The amount of humanitarian financing contributed by the U.K. is a result of the official development assistance target of 0.7% of gross national income [178]. In 2015, that amounted to the U.K. spending £12.1bn [179], a degree of funding that has received much criticism. For example, while giving evidence to a U.S. Senate Committee on foreign relations, ex-UK Prime Minister David Cameron suggested that much of the money goes to corrupt regimes, "If what we do is just have continued programs for countries that sometimes fail year after year after year, we just keep going, maybe that's not a good use of our money" [180].

4.5.2 The Responsibilities for Aid

There have been efforts to address such criticisms. The 2016 World Humanitarian Summit (WHS) described five 'commitments to action', which outline the critical responsibilities for aid:

1. Uphold the norms that safeguard humanity by enhancing compliance and accountability to international law.
2. Implement a new approach to forced displacement so that no one is left behind.
3. Achieve gender equality and greater inclusivity.
4. Instead of replacing local systems, reinforce them so that, eventually, there is no need for aid.

5. Invest in humanity by diversifying the resource base and increasing cost-efficiency [181].

The WHS described those five critical responsibilities as an 'Agenda for Humanity'[15], whose aim was to transform the lives of 130 million people living in crisis-affected areas around the world 181]. As a result, large humanitarian donors and aid organisations agreed to a *Grand Bargain* (GB) to improve the lives of people living in fragile situations because of crises [181]. The GB made many commitments, including enhancing the transparency of mutual aid reporting, thereby strengthening accountability, helping decision-making and ultimately, improving the effectiveness of humanitarian efforts. The Inter-Agency Standing Committee (IASC), a forum that was founded by UN and non-UN humanitarian partners in 1992 to strengthen mutual assistance, formed a 'workstream' to carry out the GB's transparency commitment[16]. The workstream's baseline report acknowledged that, while more information on aid funding had become available, there was still a need for more organisations to produce better quality humanitarian data [182].

4.5.3 The International Aid Transparency Initiative

Consequently, the International Aid Transparency Initiative (IATI) was adopted as the United Nation's standard open-data format for documenting aid finance [182]. Established in 2008, IATI became part of the movement for improving the reporting of charitable actions. Then, in 2013, various bodies of the United Nations (UN) began hosting IATI [183], after which it became the international framework for publishing open data on development cooperation and humanitarian assistance [182]. Indeed, as of January 2017, over 500 humanitarian organisations are using IATI, including the governments of Japan, Sweden, the U.K. and the U.S., the European Commission's Humanitarian Aid and Civil Protection department, Oxfam, Save the Children, UNICEF and the World Food Programme [183].

[15]You can read more about the Agenda for Humanity at https://www.agendaforhumanity.org

[16]The IASC Grand Bargain Workstream is available at https://interagencystandingcommittee.org/greater-transparency

4.5.4 The Financial Tracking Service

The IASC's GB workstream identified the Financial Tracking Service (FTS) of the U.N. Office for the Coordination of Humanitarian Affairs (OCHA), as the humanitarian reporting platform where IATI data from different organisations, and various platforms, could be amalgamated and published for analysis by global actors [183]. The FTS came into being in 1992 as a result of a set of guiding principles for strengthening the coordination of humanitarian emergency assistance under U.N. General Assembly Resolution 46/182[17]. As of the end of 2016, three hundred and fifty humanitarian organisations reported financial information to FTS, including all significant government donors, all U.N. humanitarian agencies, Red Cross organisations, as well as 250 NGOs and private organisations [183]. FTS can import the latest versions of the IATI standard; thus IATI complements FTS by providing the technical publishing framework by which FTS can make available structured reports on aid efforts. Despite its success, the WHS recognised that the FTS needed enhancing [184].

This thesis examines whether blockchains have capabilities that can enhance the FTS and add further succour to the transparency initiative of the WHS. It does so through the DSR artefact ReportAid, which implements IATA on the blockchain, and by so doing, provides an innovative enhancement of the UN's FTS. ReportAid is discussed in more detail in Chapter 9.

4.6 Summary

This chapter introduces the four questions that are central to this thesis, namely:

1. Can blockchains help reduce energy consumption?
2. Can blockchains help digitise the informal sector?
3. Can blockchains help counter fake news?
4. Can blockchains help address criticisms of humanitarian aid?

[17]U.N. General Assembly Resolution 46/182 is available at http://www.un.org/documents/ga/res/46/a46r182.htm

Those questions are used to examine the overarching research objective, which is whether blockchains can help humanity. That is a natural consequence of those four subordinate questions because they tackle some of the foremost challenges facing society, namely climate change, financial fraud, propaganda and corrupt use of mutual aid. Those subjects are discussed at length above.

First, this chapter gives some background that gave rise to those four questions. They are couched in the published work of this author, namely *Internet of Things, Blockchain and Shared Economy Applications* [1], *Towards a post-cash society: An application to convert fiat money into a cryptocurrency* [10], *Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains* [12] and *Socialism and the Blockchain* [11]. Those papers lay the basis for examining whether blockchain technology can go beyond economics and into other realms, an idea proposed by Swan, who defined such potential as Blockchain 1.0, 2.0 and 3.0, where 1.0 represents cryptocurrencies, 2.0 represents financial applications, and 3.0 represents applications beyond finance.

This thesis follows a similar progression when describing the DSR artefacts in this thesis. Chapter 6 describes a blockchain 1.0 cryptocurrency, Chapter 7 details a blockchain 2.0 financial application, and Chapters 8 and 9 discuss blockchain 3.0 applications beyond finance. Thus, this thesis goes further that Swan because it *realises* some of that potential of blockchains through innovative practical applications of the technology.

5 Methodology

The primary aim of this chapter is to introduce Design Science Research (DSR) as the methodological basis used to answer the overarching research question, which is whether blockchains can help humanity.

First, this chapter describes DSR and the idea of creating artefacts that enable understanding. Then it introduces design theory, which acts as a complement to DSR. This section then shows how this thesis uses the design theory component of DSR to describe the artefacts that are central to this thesis. Finally, this chapter describes the philosophy that informs the evaluation stage of DSR.

5.1 Design Science Research

DSR incorporates a set of analytical techniques for theorising about an Information System (IS) [25]. Figure 5.1, below, shows an overview of the processes involved. The general principle is to achieve an understanding of a problem by building artefacts that satisfy a set of functional requirements. The process of evaluating those artefacts then creates a mapping to a knowledge space through iterated reflection and abstraction, so the research contributes to knowledge. Therefore, although the creation of artefacts is critical, it is not the goal of DSR; instead, the focus is acquiring understanding. In that respect, DSR differs from pure design because it is the science of realisation through construction, "Knowledge is generated and accumulated through action. Doing something and judging results is the general model" [185].

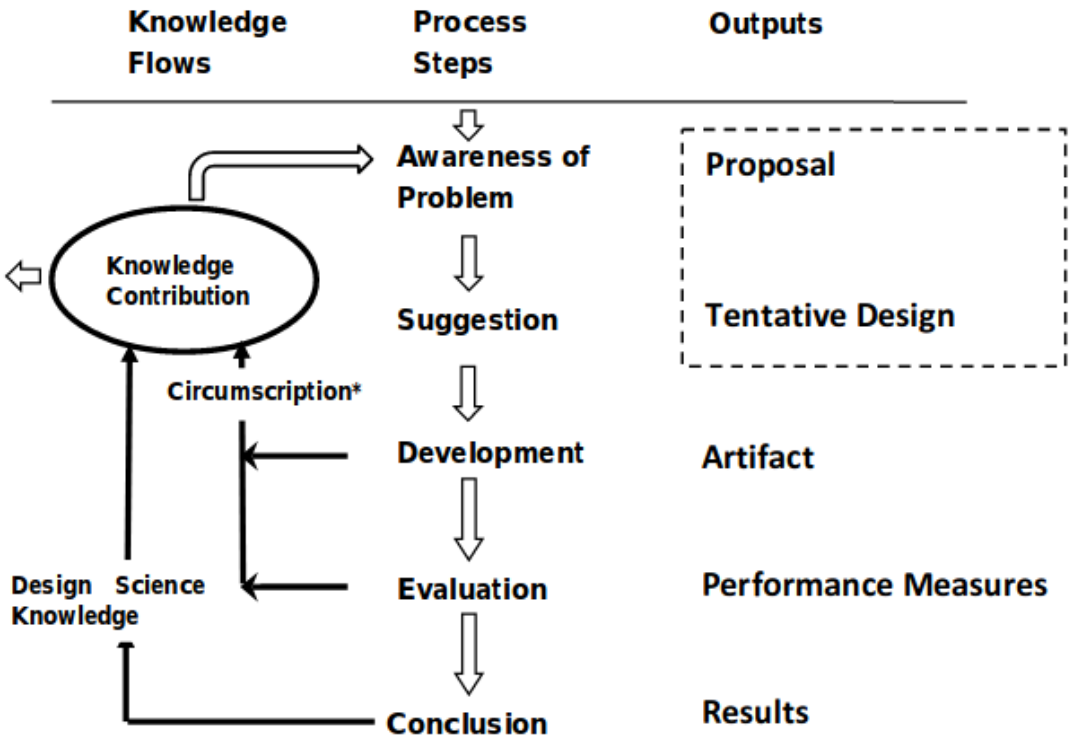


Figure 5.1: The Design Science Research Process [25]

DSR artefacts might refer to any IS object that has a physical existence [186]. Such objects could include, for example, algorithms, computer interfaces, web applications or database systems [25]. They may also include abstract artefacts, such as computer languages, diagrammatic constructs, methods or models [187].

5.2 Design Theory

Design theory (DT) complements DSR [186]; it prescribes the architecture of specific IS applications [187] by constituting a set of outcomes, upon which conclusions can be made [25]. Gregor and Jones describe eight DT components:

1. **Purpose and Scope**. First, define the intention of the system.
2. **Constructs**. A clear definition or representation of the physical entities (or abstract theories) of interest.
3. **Principles of Implementation**. How the design came into being.

4. **Principles of Form and Function**. That which defines the structure of the design. It is a type of abstract blueprint for the construction of an IS artefact.
5. **Artefact Mutability**. Consideration of how the artefact emerges and evolves.
6. **Testable Propositions**. A set of verifiable hypotheses, allowing the testing of all the stated requirements.
7. **Justificatory Knowledge**. The knowledge that links the other components; in essence, once something works, this justifies as to *why* it works.
8. **Expository Instantiation**. Help explain a design by an example, or mock-up, of the real system [187].

Those eight components are, effectively, an expansion of the first three stages of the DSR process described in Figure 5.1 above. Thus, as suggested by Gregor and Hevner [186], this thesis harmonises the DSR and DT approaches, a process that begins below with a definition of the purpose and scope of this study. Indeed, the next eight sections of this chapter apply each of those components of DT to this thesis.

5.2.1 Purpose and Scope

The objective of this thesis is to contribute to knowledge through practical demonstrations of the diverse capabilities of blockchains. The overarching aim is to answer the research question:

Can blockchains help humanity?

That question is a consequence of the author's published papers, which have focused on blockchain's ability to offer solutions to problems in finance and beyond. Chapter 4 describes those problems in more detail.

5.2.2 Constructs

Gregor and Hevner describe three levels of DSR contribution types [186]. The first level includes software artefacts. The second level involves

constructs or models that represent nascent theory. The third level constitutes well-developed theories about embedded phenomena.

This thesis describes software artefacts at Gregor and Hevner's first level of DSR contribution.

5.2.3 Principles of Implementation

The artefacts introduced above were created using methods from lean software development (LDP), which is an *agile* build methodology that borrows ideas from the Toyota Product Development System [188]. LDP was popularised in the early 2000s, with the publication of the book of the same name [188]; however, its foundations date back to the mid-1980s, when researchers began to notice the similarities between Microsoft's process of daily builds and Toyota's just in time (JIT) philosophy, whereby their production assembly line was stopped so identified problems could be fixed immediately [189].

LDP emphasises the benefits of a lightweight development style that focuses on flexibility through seven fundamental principles:

1. **Optimise the Whole**. Design, development and deployment are all critical to the success of any application.
2. **Eliminate Waste**. Eliminate anything that does not add value (or knowledge).
3. **Build in Quality**. Best practice means that systems continuously integrate small units of well-built software.
4. **Learn Constantly**. Development is all about creating knowledge. Thus, lean software development fits particularly well with DSR, since constant learning concurs with DSR's goal of acquiring knowledge through building artefacts.
5. **Deliver Quickly**. Rather than considering software development as a project, consider it as an information flow of frequent releases.
6. **Engage Everyone**. Application development should include customers, sales, marketing, designers, developers, testers,

operations, support, accountants and anyone and everyone who has a stake in the software's success.

7. **Keep Getting Better**. Any proposal is merely a starting point to be improved because at any given time the best solution will seldom remain so [189].

Lean software development fits well with design science research. For example, principles such as build in quality, always learn and deliver quickly agree with DSR's goal of acquiring knowledge through iterated reflection and abstraction of artefacts. Indeed, the seven fundamental principles outlined above are best supported by problem-solving through frequent iterations of build, measure and learn [190]. Often, LDP creates a minimum viable product (MVP), which is an application that is, "complete enough to demonstrate the value it brings" [24]. In a production setting, an MVP begins the process of learning because it has enough features to demonstrate a solution that is brought to market. However, in this context, the goal is to examine the research objective. Hence, rather than MVPs, the emphasis is to provide DSR artefacts that contribute to knowledge. This thesis builds five types of artefact, which are introduced in the Constructs section, above, and described in greater detail in the ensuing chapters.

The Kanban system is ideally suited to LDP's idea of software development as an information flow. Columns represent significant actions in Kanban-supported application development, and cards in those columns depict the current state of the work. When a card is complete, it is placed in the column to its immediate right; hence, a Kanban board represents an information flow of the system build [189]. Figure 5.2, below, shows the Kanban board used during the development of one of the DSR artefacts described in this thesis - Provenator. It demonstrates the LDP principle of building in quality via the frequent release of small units of the system as a whole since it shows distinct functional components that can be tested.

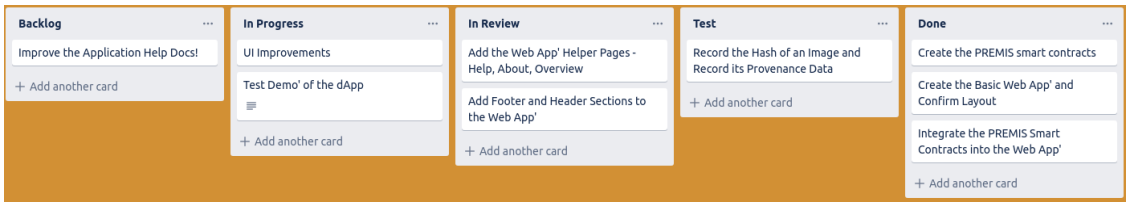


Figure 5.2: The Provenator Kanban Board

5.2.4 Principles of Form and Function

The design, form and function of each of the DSR artefacts included in this thesis is discussed in subsequent chapters:

- Enervator, and Eneradmin are discussed in Chapter 6
- Enerchanger, which is discussed in Chapter 7
- Provenator is discussed in Chapter 8
- ReportAid is discussed in Chapter 9

5.2.5 Artefact Mutability

In the context of DSR, the artefacts developed in this thesis are at the beginning of an iterative life-cycle that produces more research. Hence, this thesis allows for mutability because although the artefacts produced are used to examine the overarching research objective, they also exhibit behaviours to be developed further. Indeed, the conclusion to this thesis considers future work.

5.2.6 Testable Propositions

This work examines the research objective, which is whether blockchains can help humanity. That overarching question is examined through the lens of four additional questions, namely:

1. Can blockchains help reduce energy consumption?
2. Can blockchains help digitise the informal sector?
3. Can blockchains help counter fake news?
4. Can blockchains help address criticisms of humanitarian aid?

Chapter 6 includes examples of the use of Enervator, the cryptocurrency aimed at incentivising energy efficiency, thereby allowing testing of the first question. Enerchanger is a tool that enables the exchange of sovereign currencies for Enervator. Examples of Enerchanger in use are included in Chapter 7, thereby allowing testing of the second question. Provenator is a tool for proving the provenance of digital media. Examples of its use are included in Chapter 8, thereby allowing testing of the third question. ReportAid is an application for humanitarian aid reporting. Examples of its use are discussed in Chapter 9, thereby allowing testing of the fourth question.

5.2.7 Justificatory Knowledge

The overarching research question as to whether blockchains can help humanity is addressed through the problems described in Chapter 4. Indeed, that chapter sets the scene that justifies the research objective of this thesis.

However, much of the background to this work was grounded in the author's previously published papers. For example, the author's paper, *Internet of Things, Blockchain and Shared Economy Applications* [1], creates scenarios that propose blockchains as a tool that enables people to participate in a shared digital economy. Sharing and how society collaborates is an underlying theme of this thesis, and Chapter 3 proposes that commons-based peer production (CBPP), the method used to produce Bitcoin and blockchain technology, is how humanity can cooperate more fairly. Indeed, that was also a theme explored in *Socialism and the Blockchain* [11], which argues that the properties of blockchains make it an ideal tool for supporting Socialist societies.

Towards a post-cash society: An application to convert fiat money into a cryptocurrency [10], begins the process of realising the scenarios in *Internet of Things, Blockchain and Shared Economy Applications* [1]. It describes MicroMorpher, a tool that converts sovereign currencies into Ether. Sovereign currency to cryptocurrency conversion forms the basis of

Chapter 7, which describes Enerchanger, a tool for converting sovereign currencies into EOR.

Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains [12], implements another of those scenarios when it describes Provenator, the focus of Chapter 8, which is a DSR artefact that examines blockchain's potential for proving the provenance of digital media. *Socialism and the Blockchain* also includes a description of a cryptocurrency token that establishes its value by quantifying the amount of energy used to create that token [11]. That forms the basis of Enervator, the cryptocurrency that incentivises energy efficiency, which forms the basis of discussion in Chapter 6.

5.2.8 Expository Instantiation

The following chapters include screenshots of the DSR artefacts described in this thesis. Figure 5.3, below, gives a sample of what is to come in Chapter 7; it shows Enerchanger exchanging Rupees for EOR.

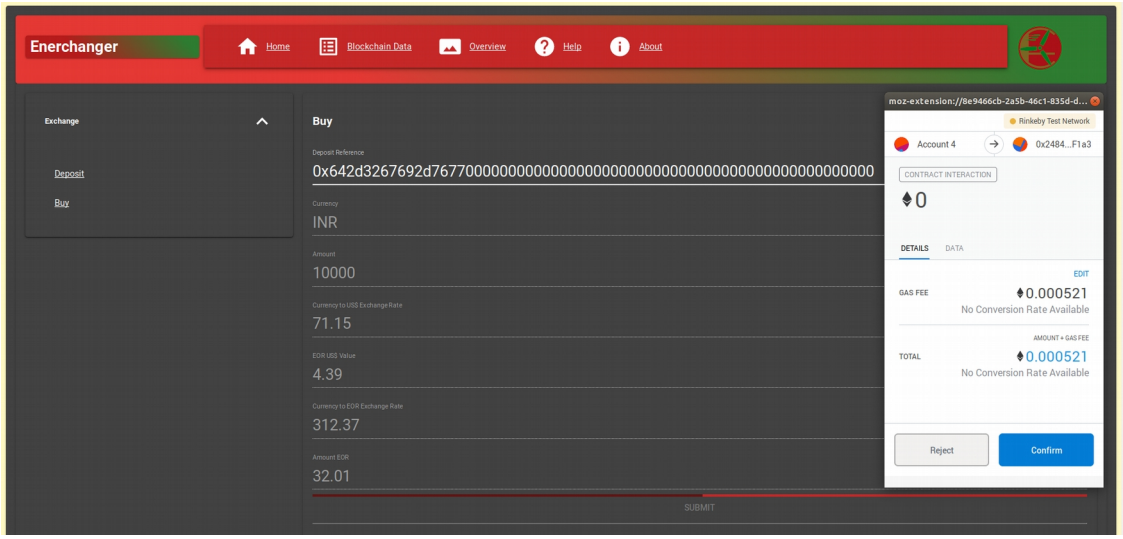


Figure 5.4: Enerchanger exchanging 10,000 Rupees for 32.01 EOR

5.3 Evaluation and Conclusion

Evaluation of the artefacts described in this thesis, which constitutes the analysis stages of DSR, begins in the following chapters; what follows below is an introduction to the philosophical foundations of that analysis.

Appendix C gives a general introduction to many of the philosophical concepts discussed.

5.3.1 Philosophical Paradigms

Vaishnavi et al. argue that the DSR researcher travels through multiple philosophical paradigms. Figure 5.1, above, shows they attribute particular importance to *knowing through making* and the process of *iterative circumscription*, whereby understanding emerges through iterating the construction of created artefacts [25]. Such novel artefacts require the DSR researcher to become comfortable with alternative worlds, which tends to exclude a wholly positivist philosophy that typically analyses a system composed of a single, composite socio-technical unit. Ontologically, Vaishnavi et al. argue that, although DSR shares similarities with the processes of interpretivism, it differs from that philosophy because it relies on abductive processes that eventually reveal a single, stable, underlying physical reality, not multiple subjective realities. However, a progressive realisation of system behaviour comes as the functionality becomes increasingly apparent as artefacts come into being. Therefore, such a process must inform (modify) the research perspective of the system as a whole [25]. Axiologically that requires the design science researcher to value ambiguous creativity over and above the more traditional research values of absolute truth and understanding [186]. Thus, the researcher welcomes the fallibility of constructivist perception, and during the abduction phase, they willingly become positivist when hypothesising about system behaviour. They then turn interpretivist once observation of the designed system begins, which resets the whole research perspective.

5.3.2 Critical Realism

Gregor and Jones suggest that design theory depends on a realist ontology because, even though the goal of DSR is a physical manifestation of constructed artefacts, the theory itself exists objectively in an abstract world [187]. Mingers shows that an IS synthesises the ontology of realism with the epistemology of a socially conditioned relativism [191]. Hence, Mingers believes Bhaskar's critical realism is ideally suited to theorising

about such systems because human-made constructs serve as a reference to understand the real-world social constructs of humans. Such a critical realist approach needs couching in pragmatism, which recognises the context that produces the DSR artefacts. Stadler suggests that context is the oppressive status quo and domination of the existing structural patterns of the industrial economy and its production processes that are inherently centralised, monopolised and hierarchical [74]. Freire argues that the oppressed must recognise the oppressor in order to achieve transformation, thus enabling a more enriching, humane experience [75]. Chapter 3 introduces the ideas of Ostrom and Castells, who propose a transformation of the oppression of Capitalism by reconnecting with the *commons* through CBPP. They propose that will help us rediscover a traditional means of organising that resulted in prosperous societies of the past [83][79].

5.3.3 Utopianism

That idea of eclipsing the oppressive status quo also suggests Utopianism, a mode of thought that imagines a world, "that is less ugly, more beautiful, less discriminatory, more democratic, less dehumanising, and more humane" [75]. Indeed, some of the ideas proposed in the author's paper, *Socialism and the Blockchain* [11], are broadly utopian because when it describes a world that is driven by the "co-operative consensus-driven model of collaboration" [11], it dares to imagine a world that differs from the Capitalist model that predominates throughout the Western World [65]. However, despite the reality that it is Capitalism that dominates, wanting better need not be some form of aspirational fantasy. Instead, Utopianism is a form of analytical reasoning whose focus is visionary; it is not just about imagining better ways for society to function, but how to make the world otherwise [192].

Levitas discusses several advantages of utopian thinking as a method [192]. Foremost is its separation from institutional normalities, which allow it to imagine, unconstrained, theoretical alternatives to the present. Indeed, by envisioning alternatives, Utopianism engenders critical

democratic discourse about what constitutes, "a just, equitable and sustainable society" [192].

Furthermore, a consideration of 'otherwise' allows the researcher to contemplate their role in society; thus, Utopianism fires the researcher's imagination, allowing their skills and capabilities to flourish because a mind without bounds knows no limits. For McKenna, the most crucial aspect of Utopianism is not its vision of some form of idealised end-state (because utopia itself may be imperfect and subject to difficulties and faults), but rather, its idea of transformation and the possibility of change [193]. Furthermore, it is not just society that evolves, but the researcher, too. That belongs to the radical change perspective because it challenges existing structures and offers insights that might enable alternatives [194].

The proposition of this thesis, of course, is that blockchain technology is one of the tools that may help construct that alternative, because it engenders the ideas of CBPP, which Chapter 3 suggests is how society may collaborate in a manner that is much more egalitarian than how Capitalism operates.

5.3.4 Pragmatism

Pragmatism could be considered as using what works, whereas utopian thinking might be conceived as dreaming [193]. Therefore, a superficial understanding would consider the two as contradictory. However, that would be a mistake because the two philosophies are connected; Utopianism analyses theoretical societies, while pragmatism blends that theory with practice. A pragmatist guided by Utopianism is forced to consider the future as a guide to understanding the past and informing the present. Thus, to a pragmatist, Utopianism is the means of transformation. The reverse is true, too, because a utopian thinker informed by pragmatism can create a future based on a critique of the past and present, "Critical engagement with the world allows us to begin to see new and more complex relationships between various aspects of existence and our horizons of experience begin to expand. As the horizon expands, the possibilities of the future become more numerous" [193].

This thesis blends Utopianism with pragmatism because, while Chapter 3 elicits the ideals of CBPP principles, the five DSR artefacts that form the core of this work, which are described in more detail in the chapters to come, provide working applications of those ideals.

5.3.5 Feminism

Although the author of this thesis is a white, British, middle-aged, middle-class, cis-gendered male, this work also conforms to a feminist ontology. After all, feminism is a just cause to which all right-minded people, no matter what their background, must surely align. Consider the MeToo movement[18], which has the aim, "to help survivors of sexual violence, particularly Black women and girls, and other young women of color [sic] from low wealth communities, find pathways to healing" [195]. The movement's Twitter campaign, #MeToo, went viral in 2017 when it was used to make public the accusation that the Hollywood producer, Harvey Weinstein, regularly abused his privilege to elicit sexual favours from vulnerable actresses. A feminist considers gender as an ongoing series of hierarchical relations and seeks to break down traditional binaries and 'Gender-as-power' [196], so the #MeToo campaign was a direct challenge to traditional male-dominated, Capitalist hierarchies. Alex Miller writes that the MeToo movement was, "an opportunity for all men to surrender their privilege and shoulder the responsibility required for gender equality" [197]. Hence, this work is feminist because it seeks to challenge top-down governance and explore whether we are best collaborating on an equal, non-hierarchical footing through CBPP, as discussed in Chapter 3 and demonstrated through the DSR artefacts described in the ensuing chapters.

5.3.6 The Philosophy of this Research

Figure 5.4, below, summarises the philosophical paradigm of this research. The arrow reflects a form of fluid re-evaluation that is suggested by the pragmatism of the critical realist who is informed by Utopianism. Hence, the approach is impossible to pinpoint because the perspective will

[18]The MeToo movement's aims and objectives are described at https://metoomvmt.org/

oscillate between different radical subjective and objective world views. A feminist ontology also forms a philosophical basis of this work because that supports the egalitarian values of CBPP and open source development, as described in Chapter 3, which the author hopes provide the foundations for a better society.

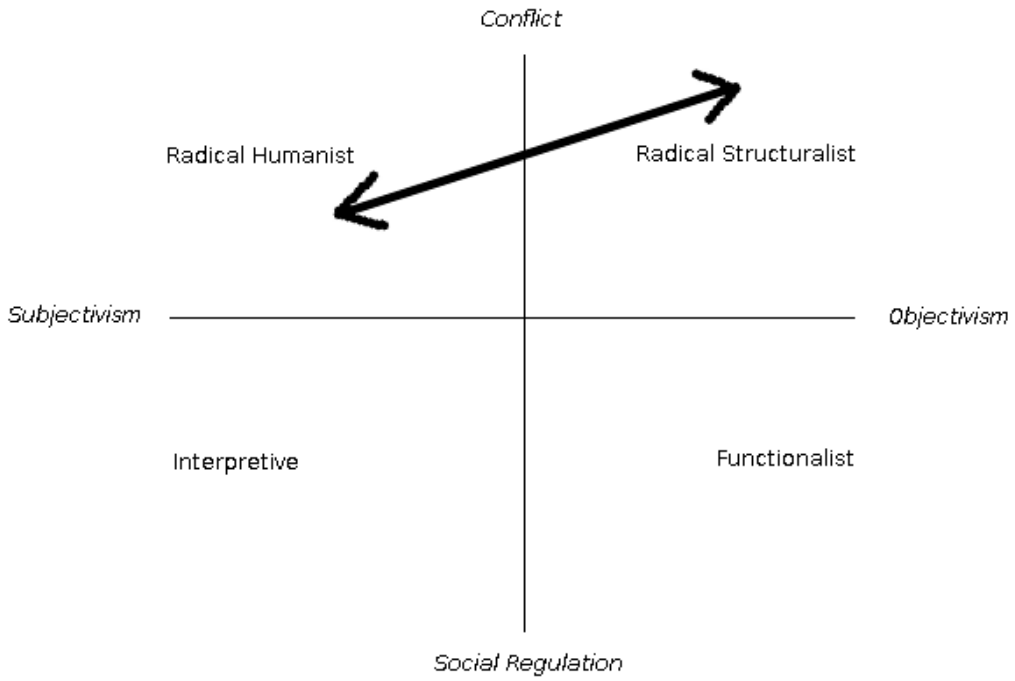


Figure 5.4: The research paradigm of this thesis [198]

5.4 Summary

This chapter describes DSR, a tool that includes a set of methods for creating knowledge through the production of artefacts. It also introduces DT, a tool that complements DSR through eight design components that are, effectively, an expansion of the first three stages of the DSR process described in Figure 5.1, above. This chapter describes those DT components at length while explaining how they pertain to the artefacts that are at the core of this thesis. Indeed, this thesis harmonises DSR and DT.

Core to this work is the DSR step, *purpose and scope*. Namely:

> *Can blockchains help humanity?*

That overarching research question is examined through the lens of four subordinate questions:

1. Can blockchains help reduce energy consumption?
2. Can blockchains help digitise the informal sector?
3. Can blockchains help counter fake news?
4. Can blockchains help address criticisms of humanitarian aid?

Those questions have their basis in the published work of this author, namely *Internet of Things, Blockchain and Shared Economy Applications* [1], *Towards a post-cash society: An application to convert fiat money into a cryptocurrency* [10], *Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains* [12] and *Socialism and the Blockchain* [11]. Those articles inspire the DSR artefacts that are at the core of this thesis. The next few chapters explain those artefacts at length. They focus, primarily, on two of the DSR steps described above; *principles of form and function*, which describes the artefacts' design, and *expository instantiation*, which shows examples of the artefacts in use. Finally, the artefacts are analysed via the *evaluation and conclusion* stages from DSR.

This chapter also described the philosophical basis of this thesis, which is broadly grounded in the philosophies of critical realism, pragmatism, utopianism and feminism.

6 Blockchains and Energy Efficiency

This thesis develops four questions that help answer the research objective as to whether blockchains can help humanity. The first of those questions asks if blockchains can help address concerns about energy consumption.

This chapter examines that first question. It does so by introducing the design science research (DSR) artefact Enervator (EOR), a cryptocurrency whose primary goal is to incentivise energy efficiency by linking its value to the inverse of global annual per capita energy consumption, thereby encouraging energy-efficient behaviour.

The name Enervator is a reference to the token's relation to energy. The word is a noun meaning 'something that enervates', where 'enervates' is a verb, meaning to weaken. Thus *Enervator* is a perfect name for a cryptocurrency whose aim is to reduce energy consumption.

First, this chapter provides some background to EOR. Then, it describes the design of EOR and discusses the mechanisms by which the token derives its value. Afterwards, the design of the DSR artefact that administers EOR, Eneradmin, is discussed, and examples of that artefact show how it is used to set the parameters that change the value of EOR. The chapter ends with an analysis of those examples.

6.1 Background

The author's paper, *Socialism and the Blockchain* [11], published in 2016, examines an innovative idea of using a digital asset to measure the value of an electric car by equating the amount of energy consumed by mining on the Bitcoin blockchain with the energy consumed over the lifetime of the vehicle. The paper contends that energy is a useful measure of value because industrial economies are increasingly mechanised. This thesis builds on that idea by proposing energy consumption as a direct measure of the price of EOR, which leads to a token that incentivises more efficient use of energy.

Socialism and the Blockchain also discusses the problem of the annual energy used by mining on the Bitcoin network, which the paper estimated as equating to the total consumption of the 2.72 million people of Jamaica [11]. During 2018, international media outlets also began noting Bitcoin's high energy demand; articles appeared in The Guardian [199], Forbes [200] and The Economist [201], to name but a few. By early November 2018, when Nature published a piece about that excessive demand [202], the author was moved to reply. He did so in an article for The Conversation, called *Bitcoin's high energy consumption is a concern – but it may be a price worth paying* [114], which concluded that Bitcoin's commons-based peer production (CBPP) practices, discussed in Chapter 3, were a rebuttal to the consumption-led ideology of Neoliberal Capitalism [114]. The piece argued that, by providing an alternative, the network might indirectly drive down the energy use of society. While that could be true, the author was left wondering if he could produce a more immediate response to those criticisms. Enervator is that response.

6.2 The Design of Enervator

This section constitutes the design theory (DT) steps of *principles of form and function* and *expository instantiation* since it outlines the blueprint for Enervator and shows numerous screenshots of the artefact in use.

Enervator is a cryptocurrency that incentivises energy efficiency. It is open-source commons-based peer production software that exists on the source code repository GitHub[19]. Figure 6.1 shows a screenshot of the homepage of that repository.

[19]Enervator is open source software, available at https://github.com/glowkeeper/Enervator

Enervator

readme style standard

A cryptocurrency stablecoin, with the token symbol EOR, whose aim is to incentivise energy efficiency.

You can read some of the details as to how Enervator incentivises energy efficiency by reading The Value of Enervator.

You can also read a Technical Overview.

**Enervator is described in more detail in Steve Huckle's PhD Thesis. Some of the information here borrows excerpts from that work.*

***The name Enervator is a reference to the token's relation to energy. The word 'enervator' is a noun meaning 'something that enervates', where 'enervates' is a verb, meaning to weaken. So in this context, the token aims to decrease energy consumption.*

Table of Contents

Figure 6.1: Enervator on GitHub

Enervator offers energy-efficiency incentives by making its value inversely proportional to consumption. Figure 6.2 outlines the use case and below describes the processes involved.

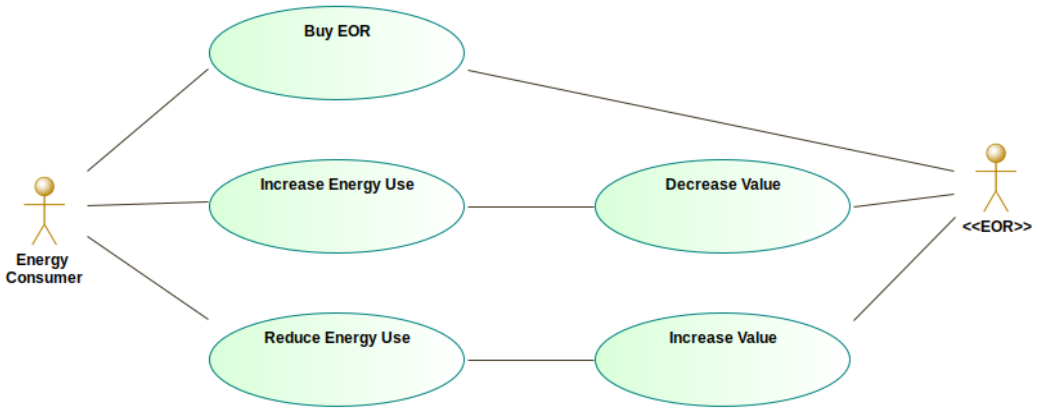


Figure 6.2: A Use Case for Enervator

6.2.1 Principles of Form and Function

The Ethereum community has developed a variety of platform standards, called Ethereum Improvement Proposals (EIPs), which include core protocol specifications, client application programming interfaces and smart contract specifications. If an EIP is approved, it becomes an Ethereum Request for Comment (ERC), which give technical guidance to standard interfaces. An example is ERC20[20], a contract interface for creating fungible assets. Fungibility is a term from economics that relates to an item's ability to be exchanged for something else; fungible goods, such as Ether or The U.S. Dollar, are equivalent and interchangeable, whereas non-fungible goods, such as deeds of ownership or collectables, are distinct [203]. Therefore, ERC20 derived contracts define tokens that represent a form of digital asset that can act as a medium of exchange on the Ethereum network; EOS[21], Augur[22] and 0x[23] are three examples of Ethereum ERC20 tokens.

The ERC777 standard maintains backwards compatibility with ERC20 but includes significant improvements. For example, it has more sophisticated mechanisms for sending and receiving tokens[24]. Figure 6.3, below, shows that Enervator inherits from OpenZeppelin's implementation of ERC777 (OpenZeppelin is a company that provides a set of production-ready contracts for Ethereum distributed application development)[25]. Enervator also includes a management contract, EnervatorManager, that holds the supply of EOR and sets the parameters that derive EOR's value. EnervatorManager also inherits from OpenZeppelin contracts, which are interfaces that enable it to send and receive tokens.

---

[20]The ERC20 token standard is described at https://github.com/ethereum/eips/issues/20

[21]EOS has the currency code EOS. You can read more about EOS at https://eos.io/

[22]Augur has the currency code REP. You can read more about Augur at https://www.augur.net/

[23]0x has the currency code ZRX. You can read more about Ox at https://0x.org/

[24]The ERC777 token standard is described at https://github.com/ethereum/eips/issues/777

[25]OpenZeppelin's ERC777 contract is defined at https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/token/ERC777/ERC777.sol

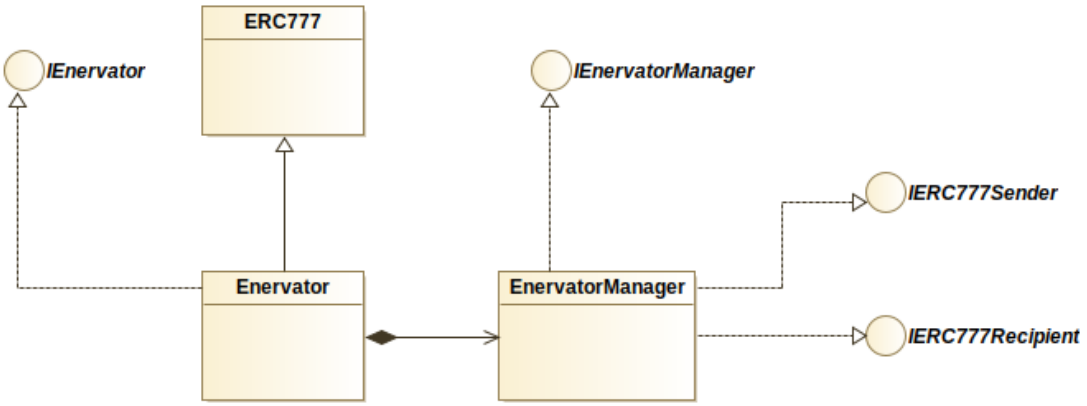


Figure 6.3: The smart contract architecture of EOR

The Ethereum smart contracts described in this thesis were all written in the object-oriented high-level language Solidity[26], whose development was supported by the Truffle suite of tools[27]. Truffle compiles each smart contract into an application binary interface (ABI), which is a compiled version of an application programming interface (API) that allows programs to call functions and use data structures from other compiled programs[28]. Truffle then links and deploys those contracts to the blockchain; for this thesis, the DSR artefacts have all been deployed to the Ethereum test blockchain Rinkeby.

At the time of writing, Enervator includes fifteen Solidity source files and 1726 lines of code. Total development time was just under two months.

6.2.1.1 Consumption Metrics

The value of EOR is to reflect two annual consumption metrics. The first is global annual per capita energy consumption (GAPCEC), which, according to figures from the World Bank, in 2014, was 1922.488 kilograms of oil equivalent, or 22.35853544 MegaWatt hours (MWh)[29].

[26]Solidity is described at https://solidity.readthedocs.io

[27]The Truffle Suite is available via https://truffleframework.com/

[28]A specification of the Solidity ABI is at https://solidity.readthedocs.io/en/v0.5.3/abi-spec.html

[29]World Bank statistics for energy use per capita are available at https://data.worldbank.org/indicator/EG.USE.PCAP.KG.OE

The second consumption metric is total primary energy supply (TPES), which, at the global level, is the sum of energy production minus storage changes. According to the International Energy Agency (IEA), in 2016, that was 13972 Megatons of oil equivalent (Mtoe), or 162,494,360,000 MWh [204].

Since the basis of the value of EOR is global energy use per capita, it seems prudent to base total supply on world population (WP). At the time of writing, that was 7,727,623,693[30].

Finally, so that it is possible to exchange sovereign currencies for EOR, a sovereign currency price per MWh is needed. Energy prices vary significantly around the world; however, figures from the IEA show that, for 2017, the global average residential electricity price (GAREP) was US$98.16 per MWh[31].

In summary:

GAPCEC = 22.35853544 MWh
TPES = 162,494,360,000 MWh
WP = 7,727,623,693
GAREP = US$98.16 per MWh

6.2.1.2 Value Algorithms

The value of EOR is to reflect energy consumption, not energy price variations, so Enervator shall use the 2017 GAREP at US$98.16 per MWh, as a constant.

A simple value algorithm would be to derive the value of a single EOR by taking the product of 2017 GAREP and GAPCEC. For example:

$$1\,EOR = 98.16 * 22.35853544 = US\$\,2194.71$$

Unfortunately, that simple algorithm rewards inefficiency, since the value of EOR would increase as consumption increases. In a world threatened by

[30] World population available at https://www.worldometers.info/world-population/

[31] IEA statistics for global average residential electricity price are available at https://www.iea.org/statistics/prices/

climate change, that is problematic. Instead, a simple fix that offers incentives for efficiency is to take the reciprocal of GAPCEC:

$$1\,EOR = 98.16 * \left(\frac{1}{22.35853544}\right) = US\$4.39$$

To further incentivise lower energy consumption, the price of a single EOR also reflects the difference between the old and the current TPES figures. To see the effect, imagine the annual TPES figures show that, unfortunately, TPES has increased from 162,494,360,000 MWh to 200,000,000,000 MWh:

$$1\,EOR = 98.16 * \left(\frac{1}{22.35853544}\right) * \left(\frac{162494360000}{200000000000}\right)$$

$$= \frac{98.16 * \left(\frac{162494360000}{200000000000}\right)}{22.35853544} = US\$3.57$$

Hence, with an increase in TPES, the value of EOR decreases, and vice versa.

6.2.2 Expository Instantiation

Next, this chapter demonstrates *expository instantiation* from DT when explaining the design of Enervator through examples [187].

At the time of writing, Enervator is available on Ethereum's Rinkeby test network[32]. Figure 6.4, below, shows Enervator on Rinkeby, shortly after its deployment; amongst the details shown are the physical address of the Enervator contract, the token supply, the number of addresses holding EOR and some initial transfers.

[32]Ethereum's Rinkeby test network is described at https://www.rinkeby.io/#stats

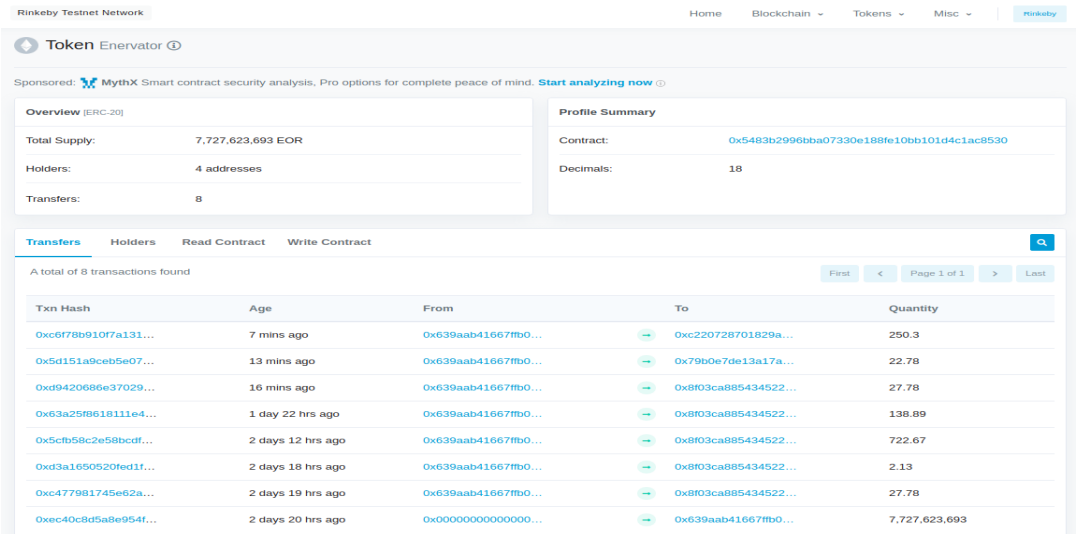


Figure 6.4: The initial deployment of EOR

The author has developed a DSR artefact to demonstrate the administration of Enervator. It is called Eneradmin[33], and it is described below.

6.3 The Design of Eneradmin

Figure 6.5 shows that Eneradmin is responsible for managing the supply of Enervator, as well as setting the token's value parameters and the sovereign currency US Dollar exchange rates. Enerchanger, the DSR artefact described in the next chapter, is responsible for converting those exchange rates into their equivalent EOR value.

[33]Eneradmin is available in the Enervator GitHub repository at https://github.com/glowkeeper/Enervator

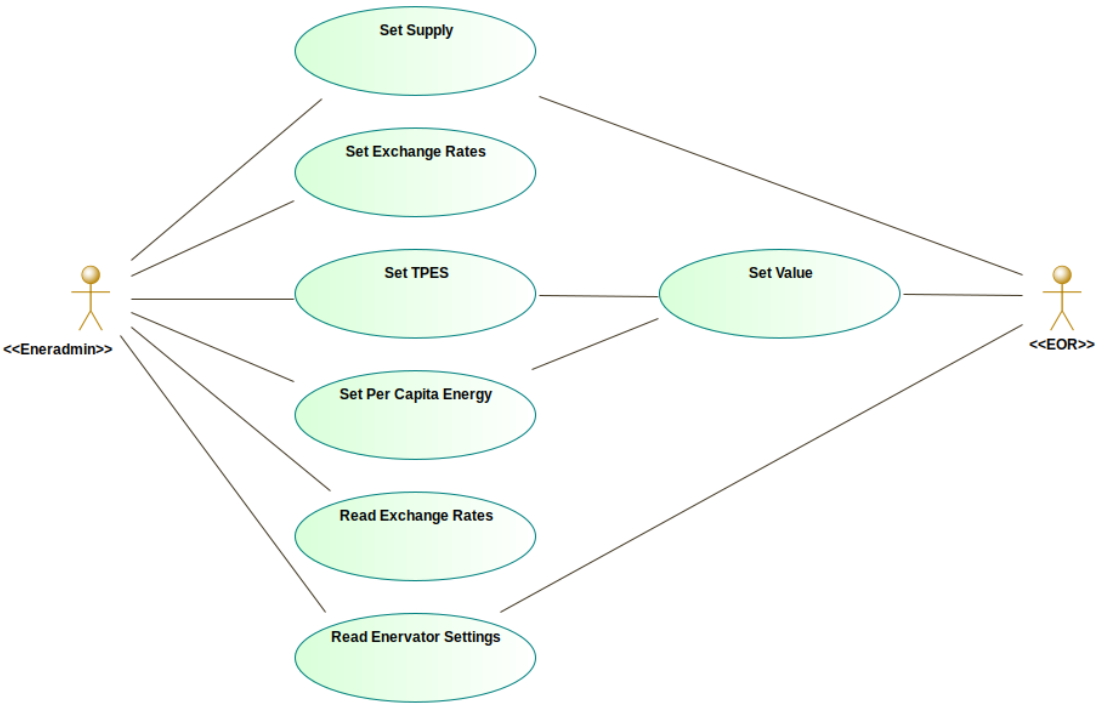


Figure 6.5: Use Case Diagram for Eneradmin

6.3.1 Principles of Form and Function

In addition to the smart contracts described in Figure 6.3, above, Figure 6.6, below, shows that Eneradmin stores and retrieves exchange rates in a Forex contract. It interacts with that contract via an Exchanger contract, which is explained in greater detail in the next chapter.

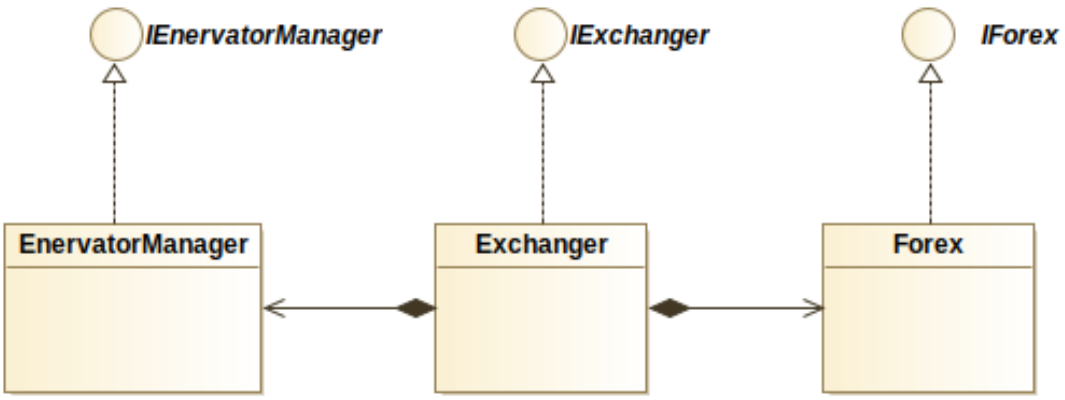


Figure 6.6: The smart contract architecture of Eneradmin

EOR, Eneradmin and the remaining DSR artefacts featured in this thesis, depends on *node.js* (or node)[34], which is a lightweight runtime environment for creating non-blocking, event-driven communication for networked Javascript web-based applications. Typically, node features numerous packages, which are managed by *npm*[35], a node package manager that helps applications form a set of publicly available, reusable node components, which are made available via application repositories, such as GitHub.

The core npm packages used by Eneradmin and the remaining DSR artefacts featured in this work were React[36], a JavaScript library for building user interfaces, and webpack[37], a tool that bundles JavaScript files, enabling their running in a web browser. Three of the four remaining artefacts (Enerchanger, Eneradmin and ReportAid) also deploy a state container in the form of React's implementation of Redux[38]. They also implement a type-safe environment through Typescript[39], a superset of JavaScript that adds static typing to variables and function interfaces.

Enerchanger, Eneradmin and ReportAid use a library called *ethers.js*[40] to access the Ethereum API, but Provenator uses *web3.js*. Whereas web3.js represents smart contracts via a JSON formatted ABI, ethers.js uses human-readable ABIs, which offers numerous advantages. However, Provenator is the eldest of the artefacts featured in this thesis, and ethers.js was not available when it was first developed. At runtime, ethers.js still uses web3.js as the underlying API provider, via MetaMask[41]. MetaMask also provides the runtime cryptocurrency wallet software that manages Ethereum accounts and thereby, allows users to sign and pay for the smart contract transactions created by Eneradmin and the other DSR artefacts featured in this thesis.

---

[34]node.js is available at https://nodejs.org/
[35]npm is available at https://www.npmjs.com
[36]React is available via https://reactjs.org/
[37]webpack is available at https://webpack.js.org/
[38]Redux is available at https://redux.js.org/
[39]TypeScript is available at https://www.typescriptlang.org/
[40]ethers.js is available at https://github.com/ethers-io/ethers.js/
[41]MetaMask is available at https://metamask.io/

At the time of writing, Eneradmin includes a total of 59 JavaScript source files and 3582 lines of code. Since Eneradmin's development was alongside that of EOR, it took the same two months of development time.

6.3.2 Expository Instantiation

Next, this chapter demonstrates *expository instantiation* from DT when explaining the design of Eneradmin through examples [187]. The scenario described below models the values described above and starts to examine whether blockchains can help address concerns about energy consumption.

Figure 6.7 shows that, at creation, EOR's total supply was 7,727,623,693 tokens, matching the global population for September 2019. It was initialised with a constant per MWh price of US$98.16, and TPES was set at 162,494,360,000 MWh. GAPCEC was set to 22.36 MWh. That results in the value of a single EOR at US$4.39:

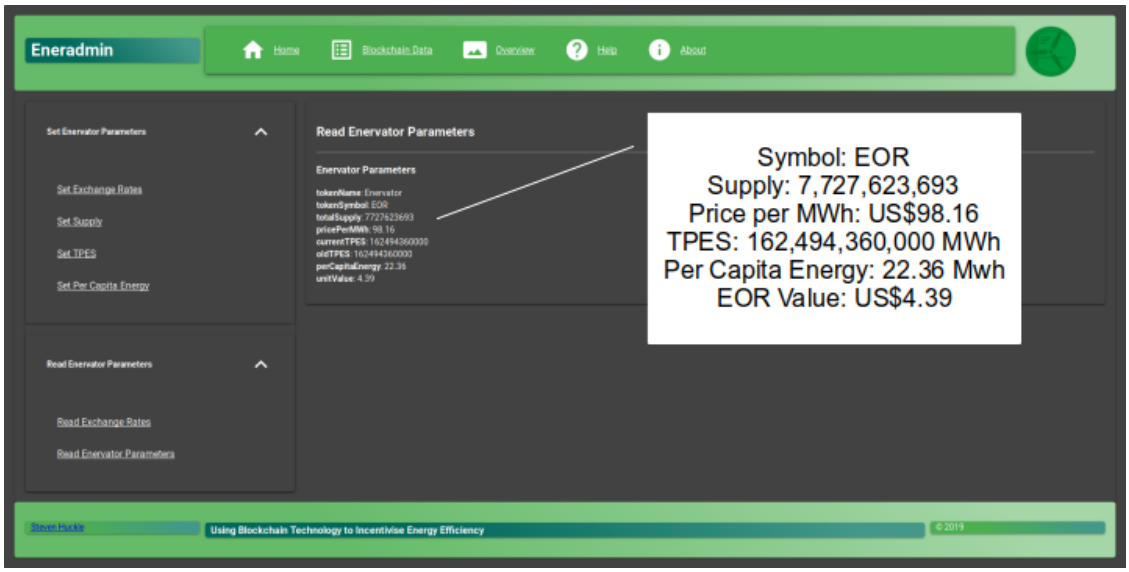


Figure 6.7: The initial value of EOR

Next, Figure 6.8 shows the author using MetaMask, via Eneradmin, to sign the transaction that changes EOR's setting for GAPCEC to 30 MWh.

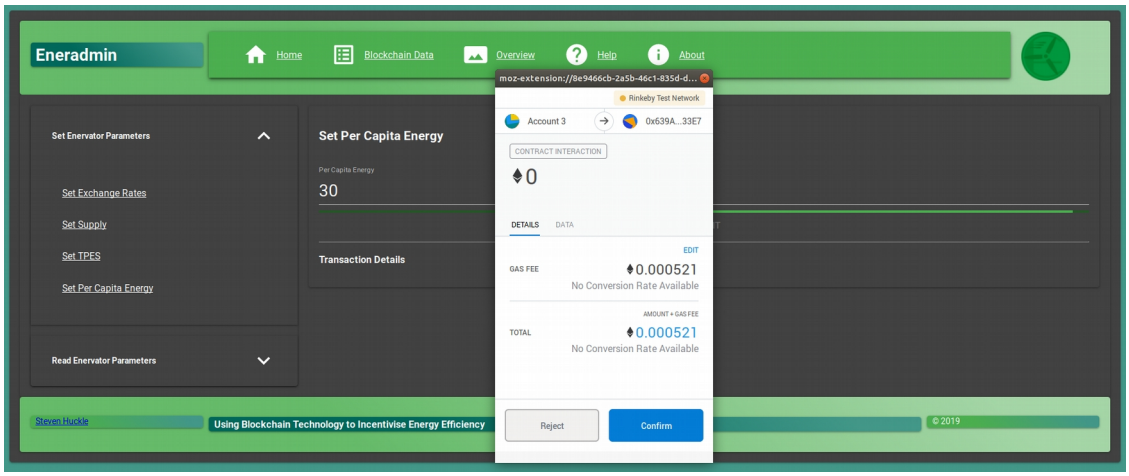


Figure 6.8: Setting per capita energy consumption at 30 MWh

Consequently, Figure 6.9 shows that EOR's value has dropped to US$3.27.

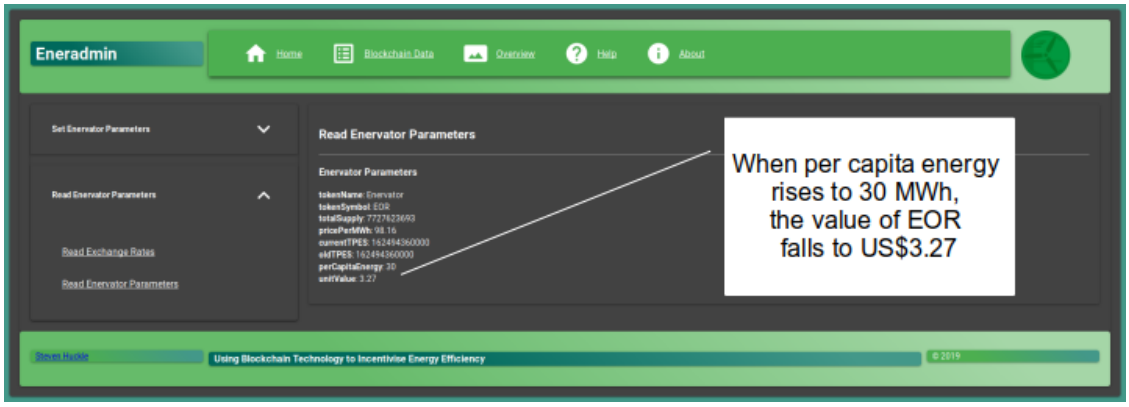


Figure 6.9: The value of EOR after setting per capita energy consumption at 30 MWh

However, Figure 6.10 shows that, if GAPCEC falls to 10 MWh, the value of EOR rises to US$9.82.

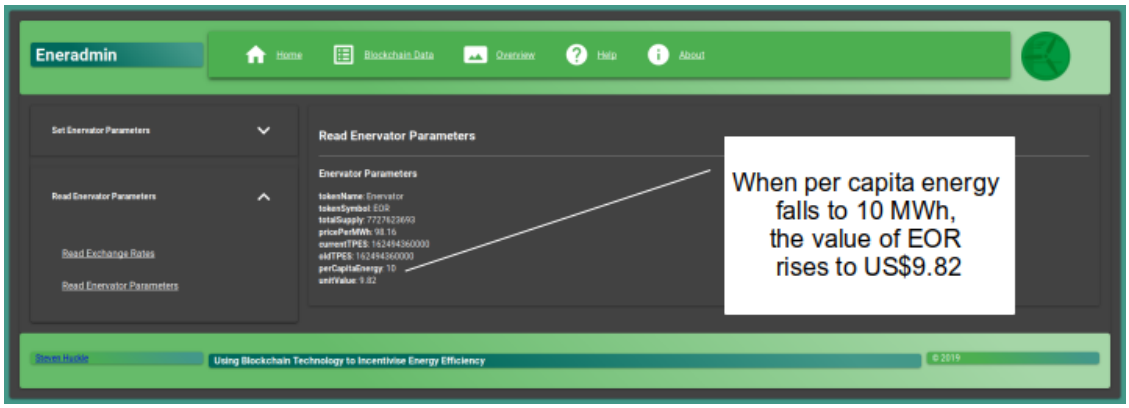


Figure 6.10: The value of EOR after setting per capita energy consumption at 10 MWh

The result is that holders of EOR have a stake in seeing GAPCEC fall, and therefore, it offers incentives for lowering their personal energy use, too.

Figures 6.11 and 6.12 show a similar mechanism for TPES. Figure 6.10 shows that with per capita energy consumption set back to its initial amount of 22.36 MWh, but annual TPES rising to 200,000,000,000 MWh, the value of EOR falls to US$3.57.

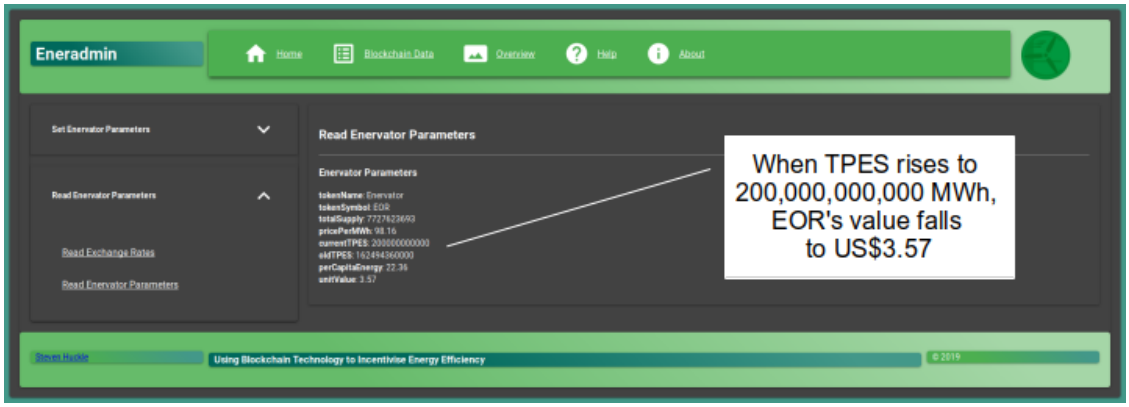


Figure 6.11: The value of EOR after setting TPES to 200,000,000,000 MWh

However, Figure 6.12 shows that, if TPES falls to 100,000,000,000 MWh instead, EOR's value rises to US$7.13.

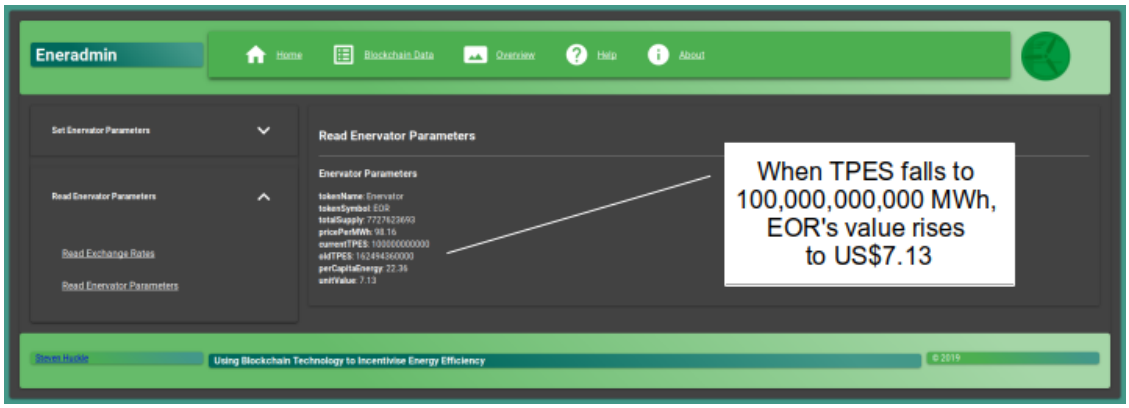


Figure 6.12: The value of EOR after setting TPES to 100,000,000,000 MWh

Hence, energy producers are similarly incentivised to decrease the amount of energy they produce.

6.4 Analysis

This analysis section constitutes the *evaluation* and *conclusion* stages from DSR. This chapter focuses on whether blockchains can help address concerns about energy consumption. The DSR artefacts Enervator and Eneradmin, described above through examples, suggest that blockchains can help incentivise people to become more energy efficient. However, there are several factors to consider before EOR can have a positive impact on energy efficiency. Those factors are discussed below.

Ultimately, since the effect of an individual lowering their consumption will have next-to-no sway on global per capita energy consumption, the success of EOR will rely on network externalities [205]. That means that there must be many token holders, but should that occur, it should amplify uptake. After all, existing holders of EOR will benefit when the number of other people holding EOR increases because that should drive the energy-efficient behaviour necessary to increase the value of the token. In turn, when people see EOR's price rising, that must result in more token holders, leading to more energy efficiencies, further increasing the value of EOR, and so on. Hence, the network effects of EOR realise the benefits of energy efficiency because its incentives help to internalise the negative external environmental impacts caused by energy consumption, consequences that

have lead to many governmental organisations around the world declaring an ecological emergency [206]. Thus, EOR offers people an opportunity to believe that their actions are no longer inconsequential in addressing climate change. That has to be positive.

Wide-scale adoption of new technologies is not without precedent. An October 2019 survey found that 2% of American adults hold Bitcoin. Additionally, a further 7.3% were planning on buying some [207]. While those numbers may not appear significant, consider that cryptocurrencies are just ten years old; when the Internet was of a similar age, global penetration was around 5.8%, whereas now, at forty years old, the Internet is used by over 50% of the planet [208].

Imagine that Wide-scale adoption does occur, and that both consumers and producers hold EOR and that their efficiencies result in the value of EOR rising. In such a case, consumers benefit directly, and producers are compensated even though consumers are no longer consuming their products. Thus, by benefiting consumers, producers and the climate, the value mechanisms of Enervator help increase 'total social welfare' [209].

6.5 Summary

The research objective of this thesis asks whether blockchains can help humanity. This chapter focuses on the first of four subordinate questions that help answer that overarching objective. It asks whether blockchains can help address concerns about energy consumption, and examines that question that through the lens of the DSR artefact Enervator, a cryptocurrency whose primary goal is to incentivise energy efficiency.

The answer to that first question is grounded in some of the author's published work - primarily, *Socialism and the Blockchain* [11], which discusses a novel idea for an energy-based cryptocurrency. That paper also expresses concern over the amount of energy consumed by mining on the Bitcoin network; a matter the author attempts to address in an article for The Conversation, *Bitcoin's high energy consumption is a concern – but it may be a price worth paying* [114]. However, whereas that article attempts a theoretical justification of Bitcoin's consumption, Enervator proposes a

practical solution that offers incentives to people to become more energy efficient.

The proposed solution offered by Enervator is examined through the DT stages of *principles of form and function*, which describes the design of EOR, and *expository instantiation*, which shows examples of how the artefact incentivises energy efficiency. Finally, this chapter uses the DSR stages of *evaluation* and *conclusion* to analyse the proposal, which suggests that EOR may positively impact energy efficiency because EOR's value has the potential to rise as consumption falls. Therefore, EOR incentivises lowering consumption. Indeed, the value mechanisms of EOR may also help increase 'total social welfare' [209] because its incentives benefit consumers, producers and the environment alike. Additionally, through internalising some existential threats to humanity's longevity caused by the climate emergency [206], EOR may help negate feelings of futility and that the environmental crisis is an insurmountable problem. However, the chapter concludes that, ultimately, EOR can only achieve all that if a significant proportion of the global population holds the token.

7 Blockchains and Digitising the Informal Sector

This thesis develops four questions that help answer the research objective as to whether blockchains can help humanity. The second of those questions examines if blockchains can help digitise the informal sector.

This chapter examines that second question. It does so by introducing the design science research (DSR) artefact Enerchanger, a blockchain-based application for converting sovereign money into the cryptocurrency Enervator (EOR), discussed in the previous chapter. By demonstrating the exchange of a sovereign currency for EOR, Enerchanger shows how blockchains can help fight financial fraud through digitising and documenting that which might have been used informally otherwise.

First, this chapter provides some background to Enerchanger[42]. Then, it describes the design of Enerchanger and discusses that artefact in an imagined scenario where it is used to support the Indian Government's drive to provide banking services to its citizens that have none. The chapter ends with an analysis of that scenario.

7.1 Background

The author first considered a novel idea for a blockchain-based currency exchange in the paper that formed the basis for this research, Internet of Things, Blockchain and Shared Economy Applications [1], which discusses the possibility of using blockchains for converting a foreign currency into its local equivalent. That idea is innovated further in the author's paper *Towards a post-cash society: An application to convert fiat money into a cryptocurrency* [10]. The paper describes the Indian Government's process of *demonetisation*, discussed in Chapter 4, which removed more than eighty per cent of India's physical cash by withdrawing 500 and 1,000 Rupee banknotes from circulation [3]. *Towards a post-cash society: An application to convert fiat money into a cryptocurrency* wonders if the

[42]Enerchanger is available in the Enervator GitHub repository at https://github.com/glowkeeper/Enervator

Indian Government could have helped the process by using the author's blockchain-based application MicroMorpher. Enerchanger is a progression of MicroMorpher.

7.2 The Design of Enerchanger

This section constitutes the design theory (DT) steps of *principles of form and function* and *expository instantiation* since it outlines the blueprint for Enerchanger and shows numerous screenshots of the artefact in use. Figure 7.1 shows a use case of Enerchanger, whereby it is responsible for taking sovereign currency deposits and exchanging those for EOR.

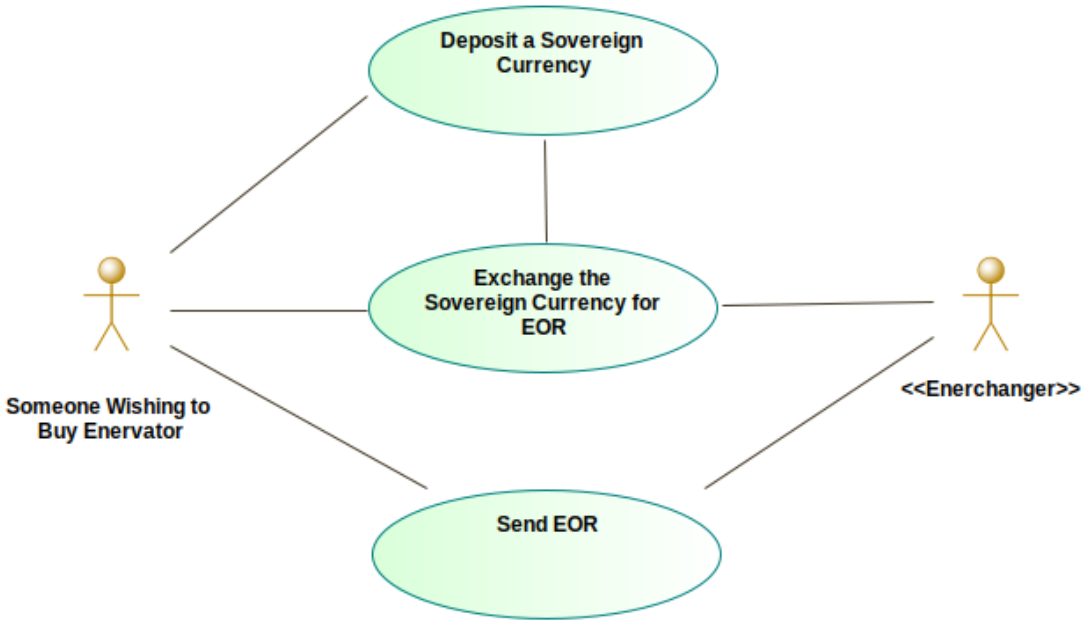


Figure 7.1: Use Case for Enerchanger

7.2.1 Principles of Form and Function

Figure 7.2, below, shows that Enerchanger retrieves exchange rates from the Forex contract in which Eneradmin, described in the previous chapter, stores those rates. It interacts with that contract via an Exchanger contract, which also interacts with contracts that store cash deposits and purchases of EOR.

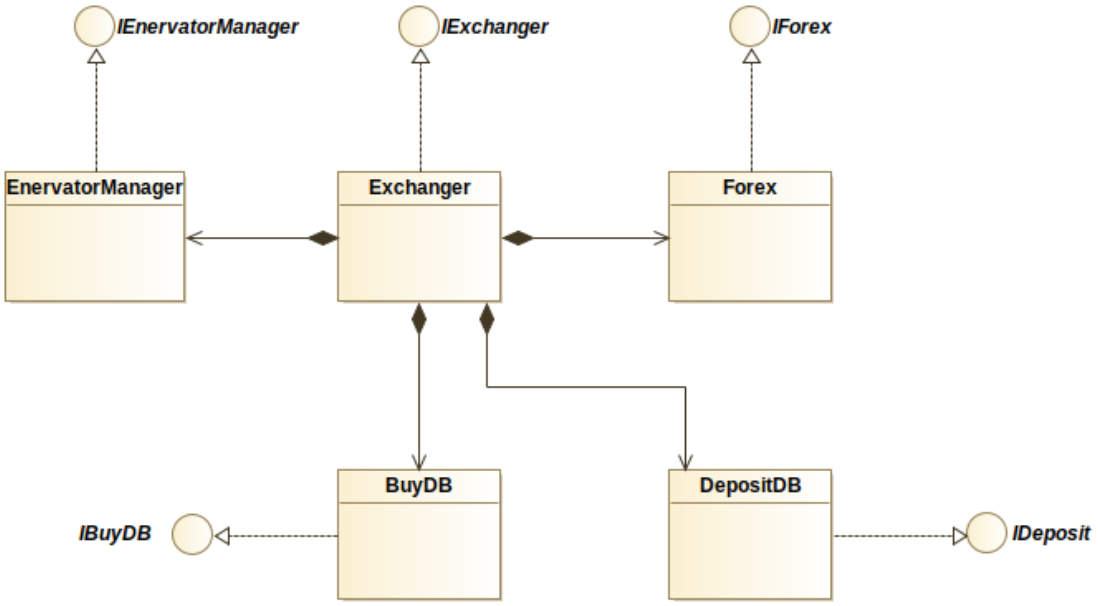


Figure 7.2: The smart contract architecture of Enerchanger

Similar to Eneradmin, Enerchanger is a web-based application that depends on the web browser extension MetaMask to provide both the access to Ethereum and the Ether to pay for the blockchain transactions that Enerchanger creates.

At the time of writing, Enerchanger includes 58 JavaScript source files and 43 typescript definition files for the smart contracts of EOR and Enerchanger. That resulted in 11791 lines of code. Development time took the same two months as that for EOR and Eneradmin. The complication of Enerchanger lies in its implementation of the ERC777 standard, discussed in Chapter 6, and its atomic send and receive mechanisms which allowed Enerchanger to update sovereign currency and EOR account balances simultaneously; ensuring the code achieves that correctly proved non-trivial.

7.2.2 Expository Instantiation

Next, this chapter employs *expository instantiation* from DT when explaining the design of Enerchanger by way of an example [187]. The scenario below begins the discussion as to whether blockchains can help

digitise the Indian informal sector. It does by imagining an Indian national exchanging her Rupees for EOR.

First, Figure 7.3, below, shows the exchange rates that Eneradmin has stored. These are the rates per U.S. Dollar, not per EOR.

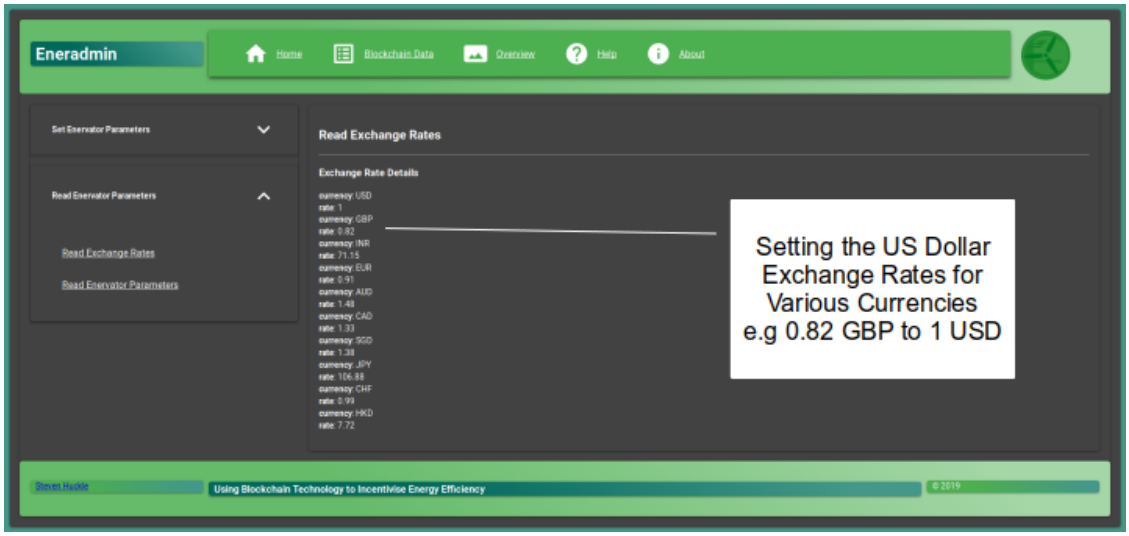


Figure 7.3: Eneradmin Exchange Rates

Next, Figure 7.4 shows a scenario whereby an Indian citizen uses the functionality of Enerchanger to deposit 10,000 Rupees, which she can later exchange for EOR. The deposit shown is a simulation of a web-based service that could easily be fulfilled by an online payment service provided by a company such as Visa, Mastercard, or PayPal.

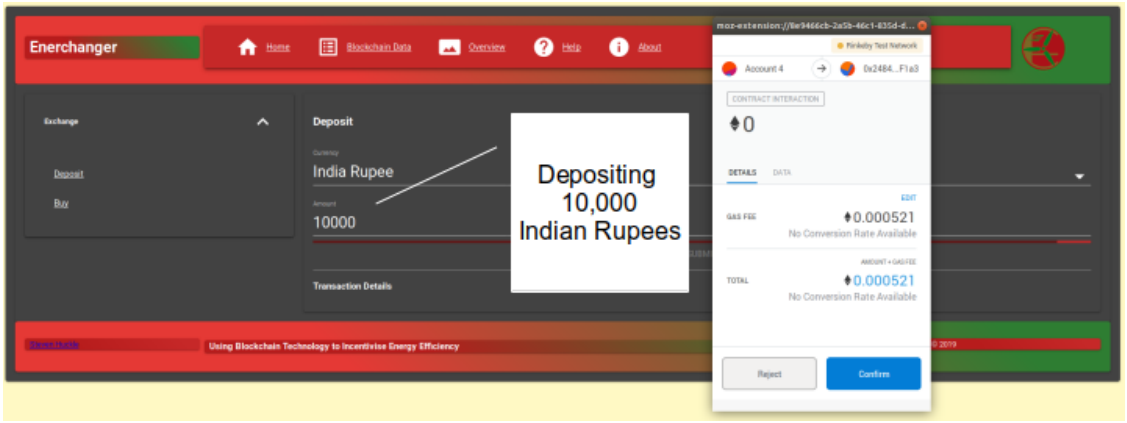


Figure 7.4: Enerchanger depositing 10,000 Rupees

Next, Figure 7.5 shows the Indian Citizen about to sign the transaction that exchanges her deposit for EOR. When buying EOR, Enerchanger displays the deposit reference, the type of currency deposited and the amount deposited. It also displays the U.S. Dollar exchange rate for that currency, the U.S. Dollar value of EOR and the deposited currency to EOR exchange rate. Finally, displayed is the amount of EOR to be bought.

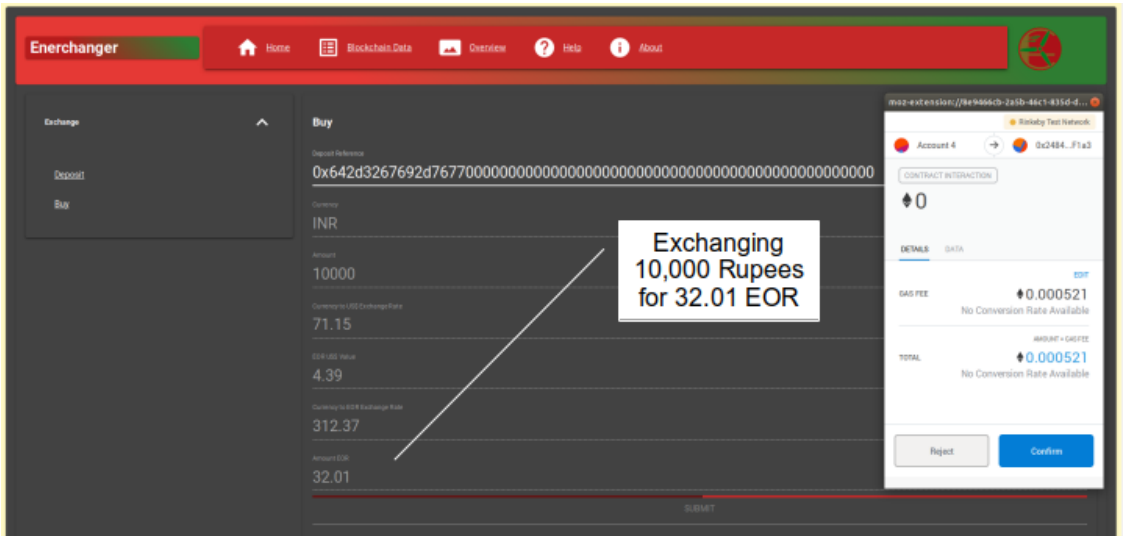


Figure 7.5: Enerchanger exchanging 10,000 Rupees for 32.01 EOR

Figure 7.6 shows the Indian Citizen's MetaMask wallet containing her newly bought 32.01 EOR.

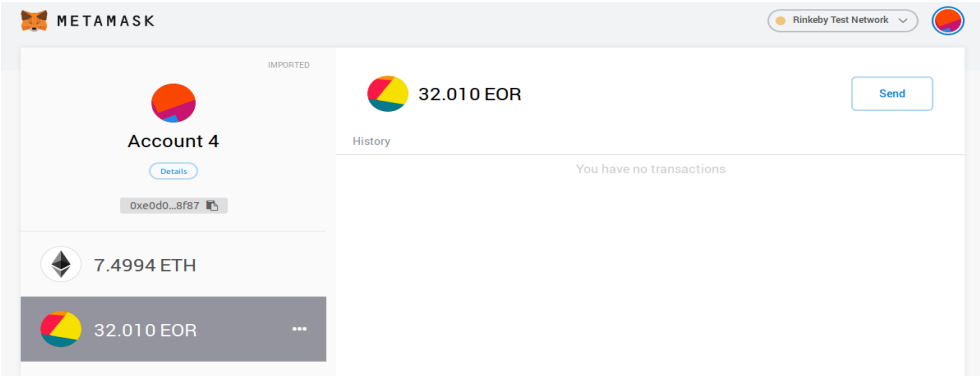


Figure 7.6: MetaMask showing the 32.01 EOR

Finally, Figure 7.7 shows that transfer on the Rinkeby blockchain explorer service, Etherscan (it is the first transfer displayed)[43].

[43]Etherscan is a blockchain explorer service for Ethereum

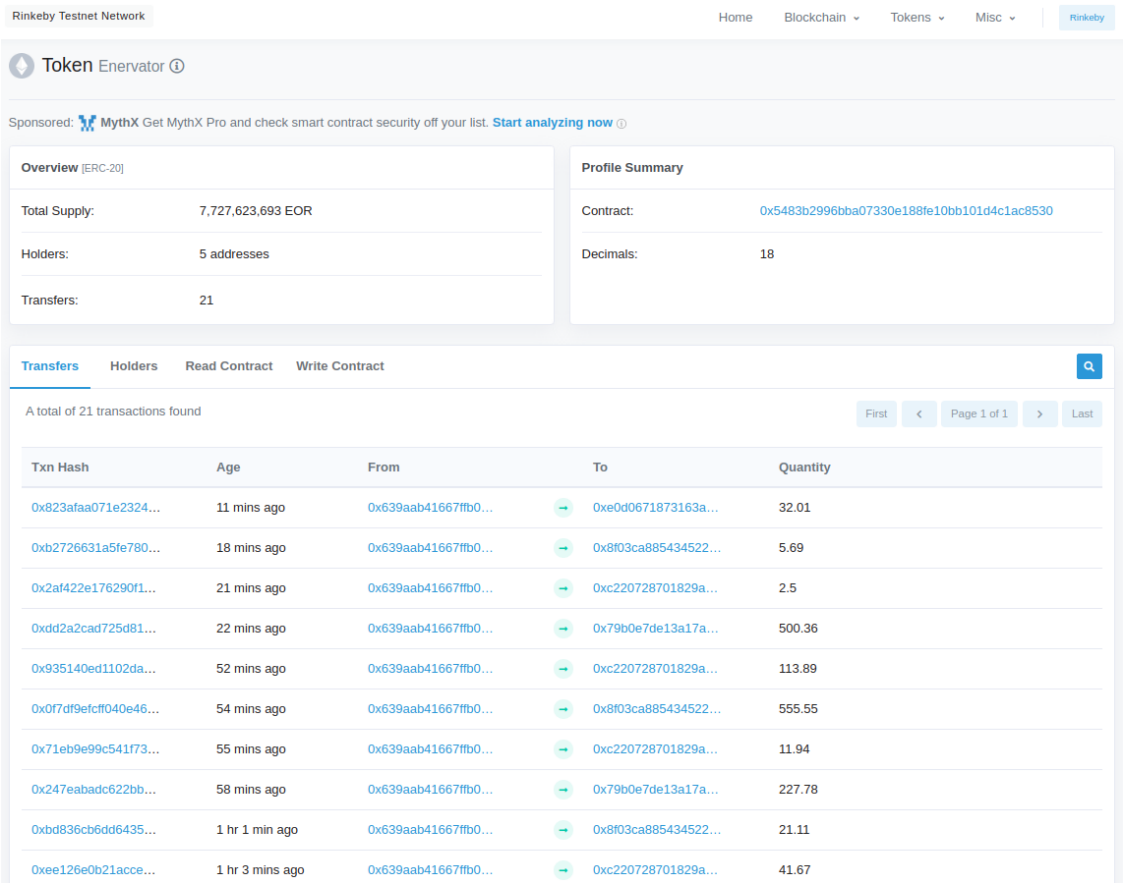


Figure 7.7: Etherscan showing the 32.01 EOR transfer

7.3 Analysis

This analysis section constitutes the *evaluation* and *conclusion* stages from DSR. This chapter focuses on whether blockchains can help digitise the informal sector. The DSR artefact Enerchanger, described above through examples, suggests that blockchains can help that financial digitisation process. However, there are several factors to consider beforehand. Those factors are discussed below.

The examples shown above show a web-based service. Unfortunately, that presupposes already digitised sovereign cash, whereas the idea is to address concerns relating to India's informal sector by helping to digitise physical cash. However, the author's paper, *Towards a post-cash society: An application to convert fiat money into a cryptocurrency* [10], imagines that the Indian Government has installed many kiosks around the country,

which are capable of accepting physical cash and converting it into Ether. Indeed, cryptocurrency based kiosks and automatic teller machines (ATM) do exist [210]. This thesis imagines ATMs for converting Rupees into EOR, whereby Figures 5.3 through 5.7 demonstrate a production version of Enerchanger running within those. Therefore, Enerchanger demonstrates the necessary functionality for digitising physical cash.

State adoption of cryptocurrencies could have many benefits. First, the decentralised nature of cryptocurrencies removes the counterparty risk of traditional sovereign currencies, where a depositor putting funds in their bank is effectively trading their cash for the bank's digital promise to redeem that deposit for the same value and to do so on-demand [211]. Martin defines such deposits as a particular type of transferable credit that creates an ephemeral and entirely cosmetic "unit of trust" [212]. That transfer relies on the clearing of credit accounts, and therefore, notes and coins are tokens of an underlying debtor relationship that is based on a pledge that is made apparent on U.K. banknotes, which declare, "I promise to pay the bearer on demand the sum of twenty pounds". Ordinarily, that promise works very well. However, it does not work quite so well in extraordinary times, when financial shocks question the viability of those units of credit. That happened in 2008 with the onset of a profound economic crisis caused by the elaborate financial schemes of a 'shadow banking sector' [213], when people around the world realised that not much certainty lay behind all the rules, regulations, and systems of sovereign cash [214]. Unfortunately, the shock caused the traditional banking sectors of many countries to show signs of financial distress, requiring state provision of direct credit support to maintain public trust in their sovereign currency [11]. By the end of 2009, the extent of international state support during the crisis was estimated to total more than US$14 trillion, or almost a quarter of the global economy [215]. Was it a coincidence that the release of Bitcoin came during the depths of that crisis, when people began to distrust traditional state-backed currencies, such as the U.S Dollar? After all, Bitcoin promised an alternative [11].

Moving physical cash into the cryptocurrency space increases the visibility and availability of financial information. Blockchains are publicly viewable,

and so all of its transactions are traceable algorithmically. Furthermore, the records are practically impossible to change [216]. An example of that traceability is shown by Figure 7.8, below, which shows EOR records held on the publicly viewable Rinkeby blockchain. It describes the address holding those 32.01 EOR, bought in Figure 7.7, above. The holder has subsequently transferred some of her tokens to other addresses - perhaps she has bought something or transferred the currency to an elderly relative living abroad. Indeed, any transaction involving that same address will feature similar transparency, which could have beneficial implications for regulators and tax authorities alike.

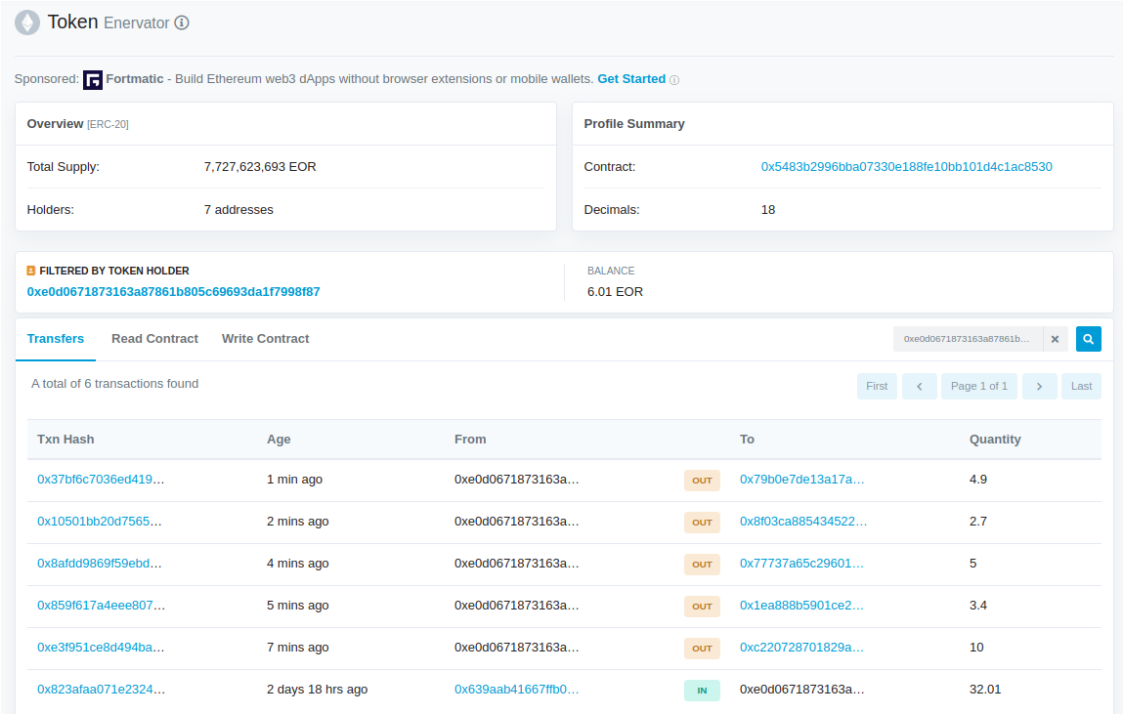


Figure 7.8: Transactions for the EOR address holding 32.01 EOR

June 2019 saw the announcement of the Libra Association (which features some of the world's largest corporations, the most prominent of which was Facebook). Their white paper published plans for a 2020 launch of a decentralised open-source blockchain, smart contract platform and low-volatility cryptocurrency called Libra [217]. The paper argues that blockchain technology has unique properties for becoming a public good because it addresses problems with financial services' accessibility and trust, issues that result in 1.7 billion adults remaining unbanked globally.

That is despite one billion of those adults having access to a mobile phone, and half-a-billion having internet access. Part of the problem lies in the high cost of money transactions, such as remittances, ATM withdrawals and loans. Libra believes its global financial infrastructure and digitally native currency can overcome such issues. It is purported to introduce stability, low inflation, global acceptance and fungibility, thus enabling, "access to better, cheaper, and open financial services — no matter who you are, where you live, what you do, or how much you have" [217]. Nakamoto's original paper on Bitcoin, which introduced the world to the idea of cryptocurrencies, made similar claims when it proposed a system for electronic transactions that negated the need for centralised systems of trust, thereby reducing transaction costs [8].

Despite the benefits cryptocurrencies offer, many countries have legislated against them. The reasons for that may be many; it could be that by allowing cryptocurrencies, governments would have to forgo *seigniorage*, which is the revenue earned by issuing the currency. That occurs in several ways, but the most important is the profit made due to differences between production and distribution costs and the value of money itself [70]. Legislation against cryptocurrencies may also be due to issues of monetary sovereignty, which is the Government's right to exercise exclusive control over the supply of currency, giving it the ability to control the nation's inflation rate and overall financial stability [10]. The importance of the nation-state retaining its ability to exercise exclusive control over the supply of currency was recognised in Ancient China, "Whoever wished to remain in power and see his domain well-governed should jealously guard the management of the monetary standard and the monopoly of issuance" [212]. The nation-state has many advantages as an issuer of money. Firstly, it conducts by far the most significant volume of economic transactions. Second, it has political authority. Finally, it has legitimacy, which is essential because sovereign money relies upon a government promise to match its value with equivalent new notes [212]. That is not to say that such legitimacy is not open to question, as has been shown above.

However, governments have already surrendered much of their sovereign power over money creation to corporate lenders [218]. Mellor explains

how, when describing the ecologically damaging debt mechanisms of Capitalism, whereby the need to repay interest on that debt drives excessive growth because it necessitates increasing productive capacity and, inevitably, that puts pressure on natural resources [218]. That relationship between debt and money creation also has repercussions for traditional function of banks, who used to profit by passing on savers' deposits to borrowers because they were able to charge debtors more interest than that given to savers. However, in the last decade, monetary authorities have acknowledged that it is a popular misconception to hold such a view of modern banks, as the direct link between savings and deposits has mostly disappeared. Instead, the lending practices of private banks create much of the new money of modern economies [219]. In that context, the announcement of the Libra cryptocurrency was fascinating; after all, it is another example of large corporations attempting to wrest control of currency issuance. It is precisely that which troubles commentators such as Clarke, who, although lauding its proposition to foster positive innovation, widen access to financial services, and give people greater control over their money, worry about ceding control to a cartel of private companies [220]. Indeed, policymakers around the world have been sceptical of the announcement of Libra. For example, French Finance Minister Bruno Le Maire confirmed this author's suspicion that it was sovereignty preventing the adoption of cryptocurrencies. He argued for legislating against Libra because it has the potential to disempower a country's ability to constrain inflation.

Nevertheless, despite reluctance, there is nascent international government support for cryptocurrencies. For example, Argentina allows people to top up their state public transport cards with Bitcoin, and the Gibraltar Blockchain Exchange allows its citizens to trade cryptocurrencies, such as Bitcoin and Ethereum [221]. In December 2017, the President of Venezuela, Nicolas Maduro, announced that the country would adopt the Petro or Petromoneda, a new national digital cryptocurrency, that would be backed by the country's natural resources, such as oil and gas [222].

Hence, governmental cryptocurrency support is not without precedent, despite consequences for monetary sovereignty. In that regard, EOR has supply mechanisms that would allow the Indian government to control inflation were it to consider the extraordinary step of adopting a version of the token as its national currency. Currently, EOR's total supply relates to the global population. However, that need not be so; there would be nothing to stop India fixing the token's supply to match the total supply of their current sovereign currency. In essence, then, this thesis proposes the Indian government adopt EOR as a sovereign currency because it would help digitise their informal sector. That idea of national cryptocurrency adoption has support elsewhere; indeed, Clarke argues that rather than relying on Libra, society needs governments to deploy their own digital currencies in the public interest [220].

7.4 Summary

The research objective of this thesis asks whether blockchains can help humanity. This chapter focuses on the second of four subordinate questions that help answer that overarching objective. It asks whether blockchains can help digitise the informal sector, a question that is examined through the lens of the DSR artefact Enerchanger, a blockchain-based application for converting sovereign money into EOR.

The answer to that second question is grounded in the author's paper *Towards a post-cash society: An application to convert fiat money into a cryptocurrency* [10], which discusses the Indian Government's process of *demonetisation*. The paper proposes that the process might have been helped by the author's blockchain-based application MicroMorpher, of which, Enerchanger is a progression.

The proposed solution offered by Enerchanger is examined through the DT stages of *principles of form and function*, which describes the design of the application, and *expository instantiation*, which shows examples of how the artefact exchanges physical cash for EOR. Finally, this chapter uses the DSR stages of *evaluation* and *conclusion* to analyse the proposal, which suggests that currency exchange, via Enerchanger, has the potential to

help digitise the informal sector and thereby, has positive implications for tackling financial fraud because EOR increases the transparency of financial transactions. It also removes the counterparty risk of traditional sovereign currencies. However, such benefits rely on governmental support for cryptocurrencies and many governments appear reluctant to provide such support, perhaps due to concerns regarding monetary sovereignty.

8 Blockchains and Fake News

This thesis develops four questions that help answer the research objective as to whether blockchains can help humanity. The third of those questions examines if blockchains can help counter fake news.

This chapter examines that third question. It does so by introducing the design science research (DSR) artefact Provenator, which is a blockchain-based application for determining the provenance of digital media. The main idea of Provenator is to use blockchains to record metadata about digital creations, thereby allowing creators to prove the origins of their works, which, amongst other uses, can help fight fake news.

First, this chapter provides some background to Provenator. Then, it describes the design of Provenator and discusses that artefact in an imagined scenario where it is used to establish the true origins of a photograph that was used to claim voting irregularities during the 2016 U.S. Presidential campaign. The chapter ends with an analysis of that scenario.

8.1 Background

The novel idea for Provenator developed in this author's paper - *Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains* [12], which described a photograph, shown below in Figure 8.1, that a supporter of Donald Trump alleged showed his opponents rigging votes. The New York Times ran a story about the picture, where they proved it was fake because instead of showing voting irregularities during the 2016 U.S. Presidential campaign, the photograph showed ballot boxes used for an earlier election in Sheldon, Birmingham, UK [223]. After considering the amount of research the New York Times must have put into their story, the author proposed an innovative blockchain solution to quickly and easily establish the origins of digital media.

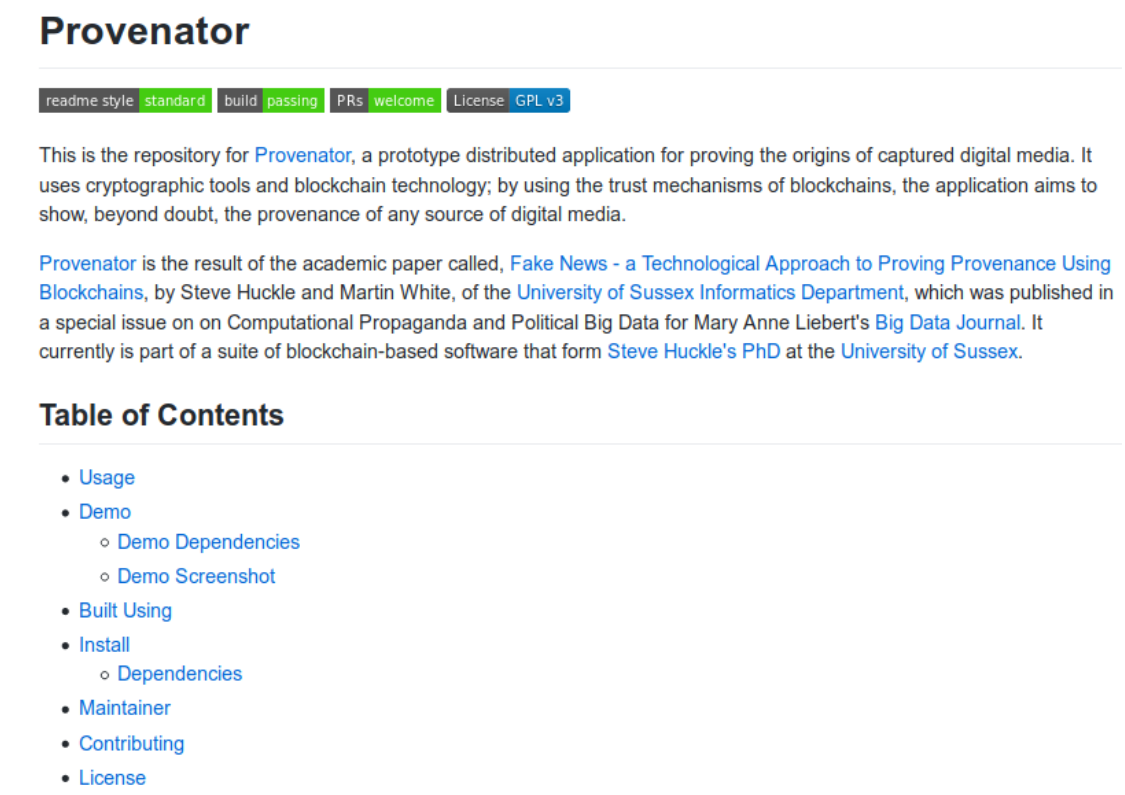
Figure 8.1: Sheldon Election Ballot Boxes [224]

8.2 The Design of Provenator

This section constitutes the design theory (DT) steps of *principles of form and function* and *expository instantiation* since it outlines the blueprint for Provenator and shows numerous screenshots of the artefact in use.

Provenator is an application for verifying the authorship and rights of digital media. It is open-source commons-based peer production software that exists on the source code repository GitHub[44]. Figure 8.2 shows a screenshot of the homepage of that repository.

[44]Provenator is available at https://github.com/glowkeeper/Provenator



Provenator

readme style standard | build passing | PRs welcome | License GPL v3

This is the repository for Provenator, a prototype distributed application for proving the origins of captured digital media. It uses cryptographic tools and blockchain technology; by using the trust mechanisms of blockchains, the application aims to show, beyond doubt, the provenance of any source of digital media.

Provenator is the result of the academic paper called, Fake News - a Technological Approach to Proving Provenance Using Blockchains, by Steve Huckle and Martin White, of the University of Sussex Informatics Department, which was published in a special issue on on Computational Propaganda and Political Big Data for Mary Anne Liebert's Big Data Journal. It currently is part of a suite of blockchain-based software that form Steve Huckle's PhD at the University of Sussex.

Table of Contents

- Usage
- Demo
  - Demo Dependencies
  - Demo Screenshot
- Built Using
- Install
  - Dependencies
- Maintainer
- Contributing
- License

Figure 8.2: Provenator on GitHub

Figure 8.3 shows a use case where digital media creators can use Provenator to store digital media provenance records of their creations. Key to the operation is generating a cryptographic hash of the media object. Because of the deterministic and collision resistance properties of cryptographic hashes, the same digital media resource always generates the same, unique hash (Appendix A includes an overview of cryptographic hashing functions). Provenator uses a KECCAK-256 hashing function[45].

[45]You can read more about the Keccak family of hashing functions at https://keccak.team/index.html

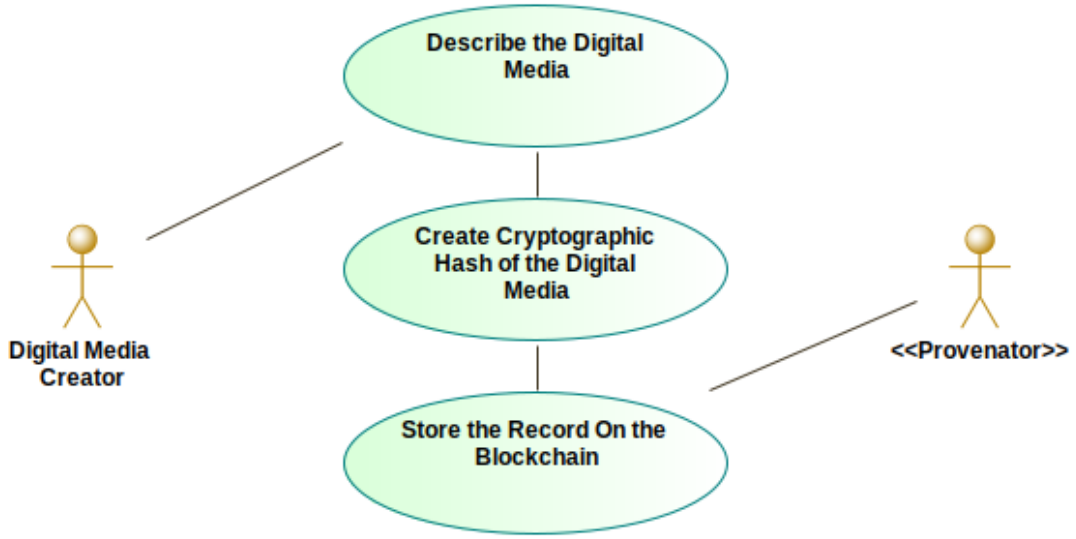


Figure 8.3: A Create Record Use Case for Provenator

Figure 8.4 shows a use case where someone creates a cryptographic hash of a digital media object, and Provenator uses that hash to retrieve the provenance of that object. Because cryptographic hashes are unique to the object being hashed, they are confident that the record retrieved relates to the object for which the hash was generated.

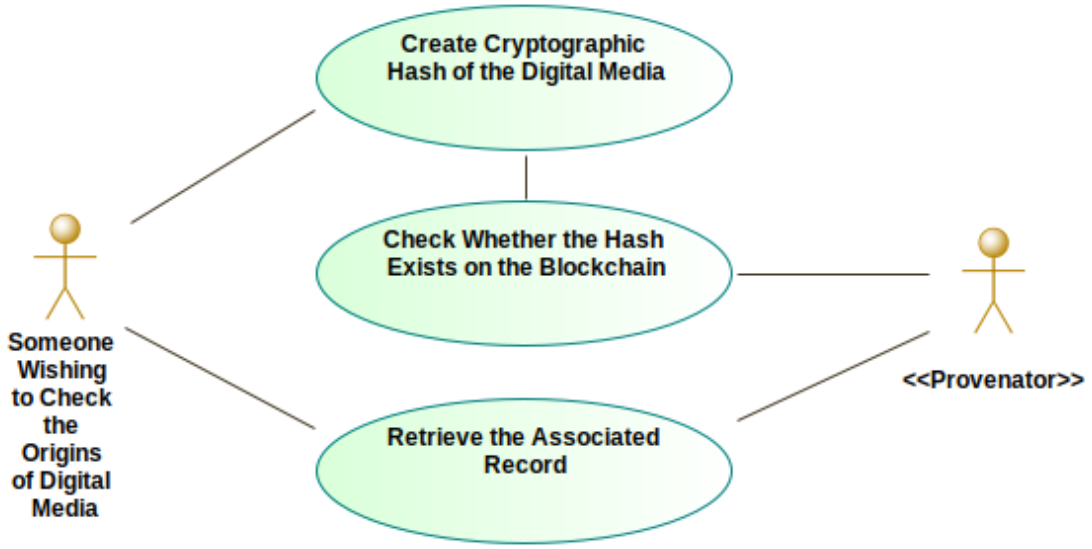


Figure 8.4: A Retrieve Record Use Case for Provenator

8.2.1 Principles of Form and Function

Provenator records PREMIS metadata definitions on the blockchain. PREMIS stands for *Preservation Metadata: Implementation Strategies*; it is an open standard that helps identify resources[46]. The PREMIS data model, shown in Figure 8.5, below, describes four separate preservation entities:

1. **Objects**. Used to record the cryptographic hash of the digital media object, as well as associated data, such as the media type.
2. **Events**. Used to record events about the digital media object. Provenator uses this entity to record the creation time of the digital media record.
3. **Agents**. Describes the digital media owner.
4. **Rights**. Describes the legalities of the object, such as its copyright.

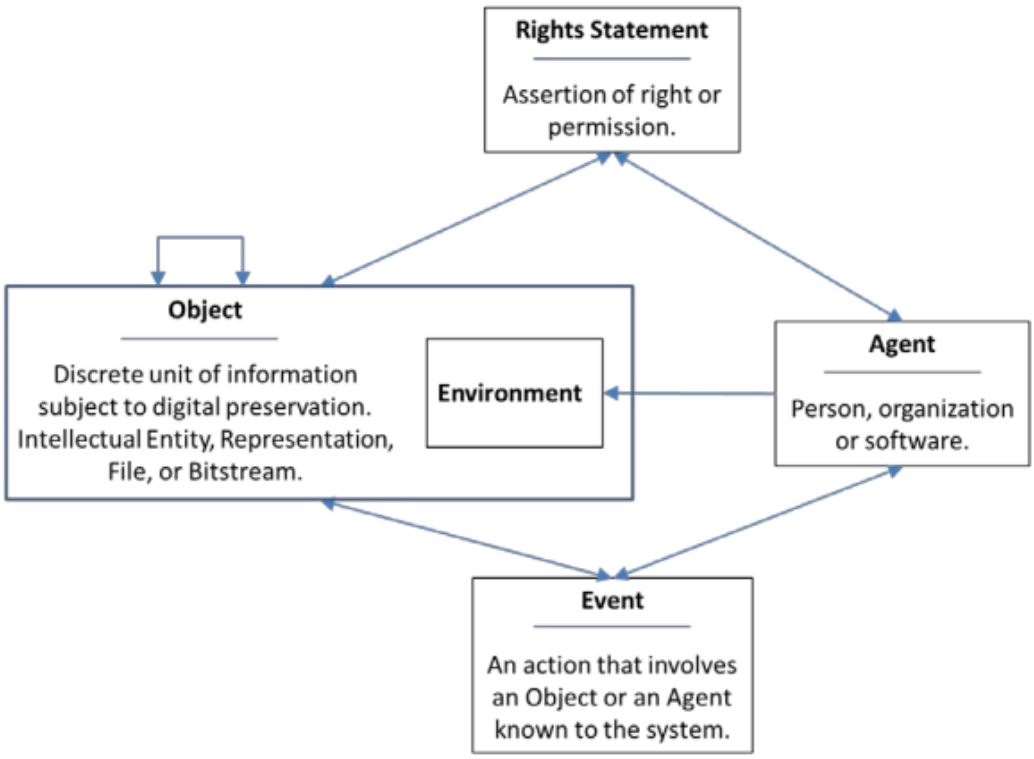


Figure 8.5: The PREMIS 3.0 data model [225]

[46]The PREMIS open standard used by this thesis is defined at https://www.loc.gov/standards/premis/v3/premis-3-0-final.pdf

Figure 8.6 shows that the smart contract architecture of Provenator mirrors that of the PREMIS 3.0 data model. By using PREMIS, Provenator ensures that it can easily share the data it stores with other users and applications [226]. Indeed, Mannens et al. propose that the use of metadata, such as PREMIS, facilitates transparency and trust [227].

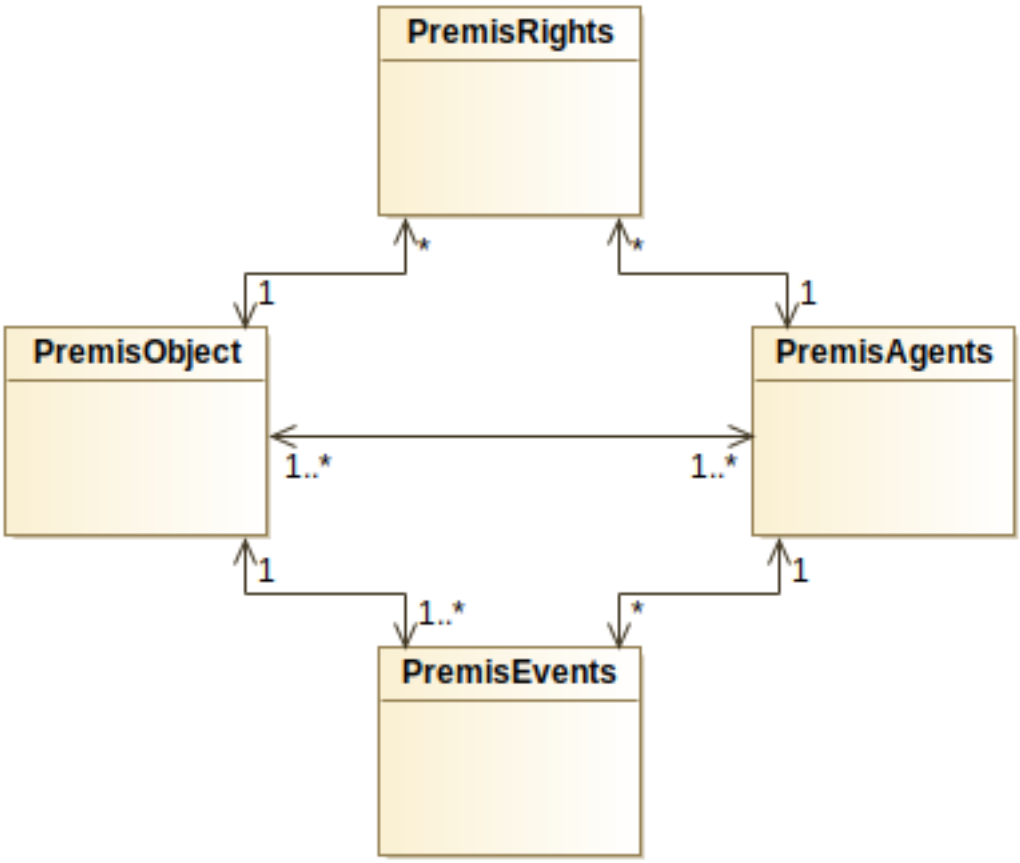


Figure 8.6: The smart contract architecture of Provenator

Similar to the applications discussed previously, Provenator is a web-based application that depends on the web browser extension MetaMask.

At the time of writing, Provenator includes a total of thirty JavaScript and ten Solidity source files, as well as 5675 lines of code. Total development time was approximately six months. Correctly porting the PREMIS standard to the blockchain proved non-trivial. Still, it served as an excellent introduction to the complications involved in implementing XML on the blockchain. That proved invaluable when it became necessary to port the

much bigger International Aid Transparency Initiative standard, which is the topic of discussion in Chapter 9.

8.2.2 Expository Instantiation

Next, this chapter employs *expository instantiation* from DT when explaining the design of Provenator by way of examples [187].

First, consider the scenario depicted in Figure 8.7, below, which shows a photograph of the author recovering after some strenuous guitar practice.

Figure 8.7: A photograph of the author recovering after a hard five minutes practice

After realising that a plethora of music magazines are going to want to display that photograph on their front cover, the author decides he should use the PREMIS architecture of Provenator to record the picture's copyright information. Figure 8.8, below, shows a screenshot of Provenator invoking MetaMask to sign the blockchain transaction that records the provenance of the photograph. Stored are the cryptographic hash of the picture, its description, the originator of the photograph and its required licensing information.

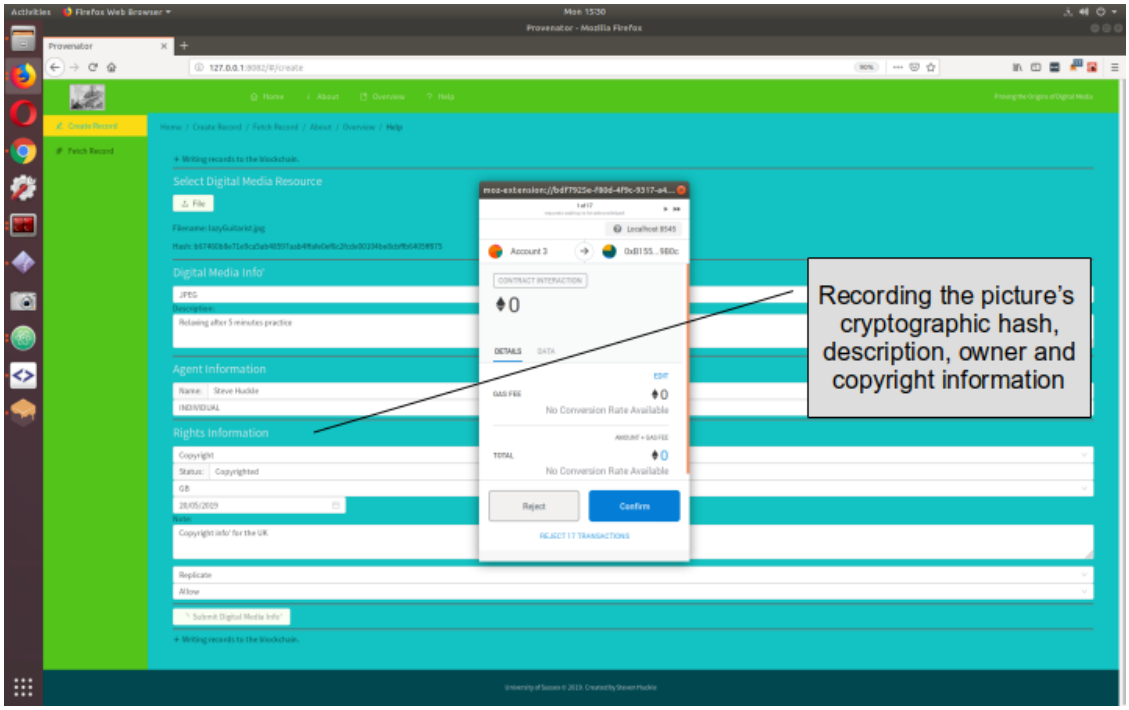


Figure 8.8: Provenator storing the provenance information of a photograph

Subsequently, any music magazine showing an interest can retrieve the picture's copyright information, only by loading it into Provenator. Figure 8.9, below, shows a screenshot of that imagined scenario.

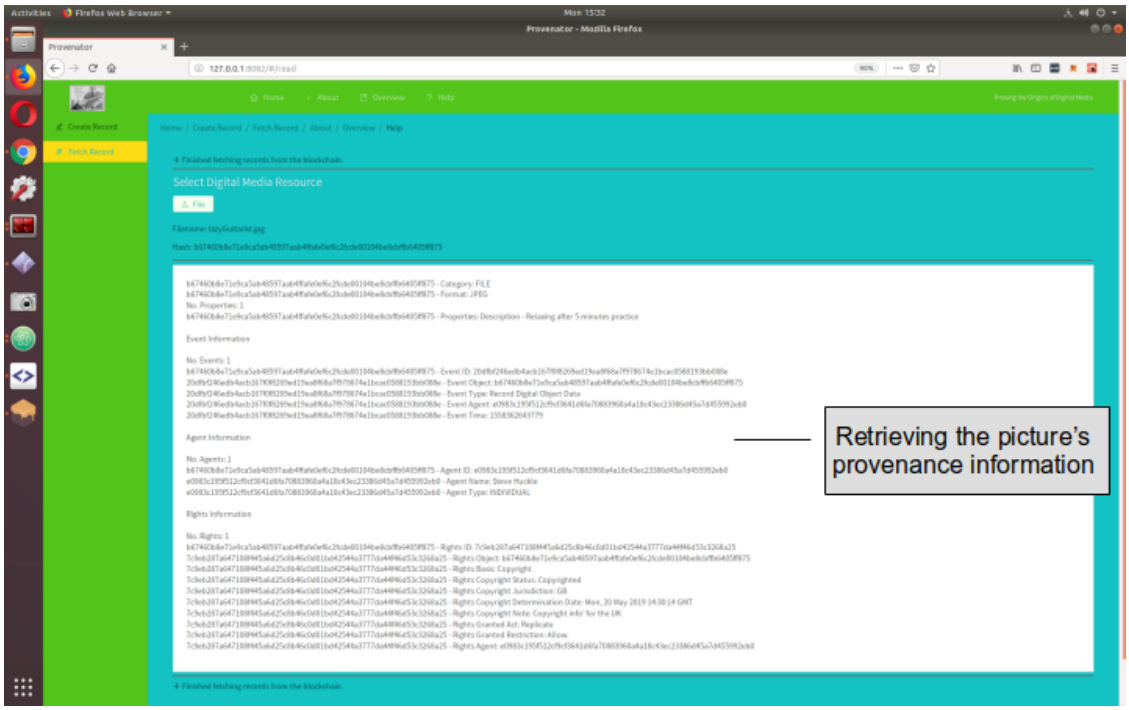


Figure 8.9: Retrieving the blockchain record of the author's picture

Next, the scenario below explores whether blockchains can counter fake news. As discussed above, this author's paper, *Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains* [12], introduces Provenator. The paper depicts a scenario whereby a Trump supporter published a photograph alongside a claim that it showed the Democrats were rigging votes during the 2016 U.S. Presidential election. In reality, the picture showed ballot boxes used for an earlier poll in Sheldon, Birmingham, UK [12]. The paper imagines Alice was the photographer of that picture of the Sheldon Election Ballot Boxes. Figure 8.10, below, shows that to register herself as the creator of that photo, Alice uses the PREMIS architecture of Provenator to store a cryptographic hash of her picture alongside its description. She also saves the date the photo was taken and establishes herself as the photographer. Finally, she records the photograph's copyright and licensing information.

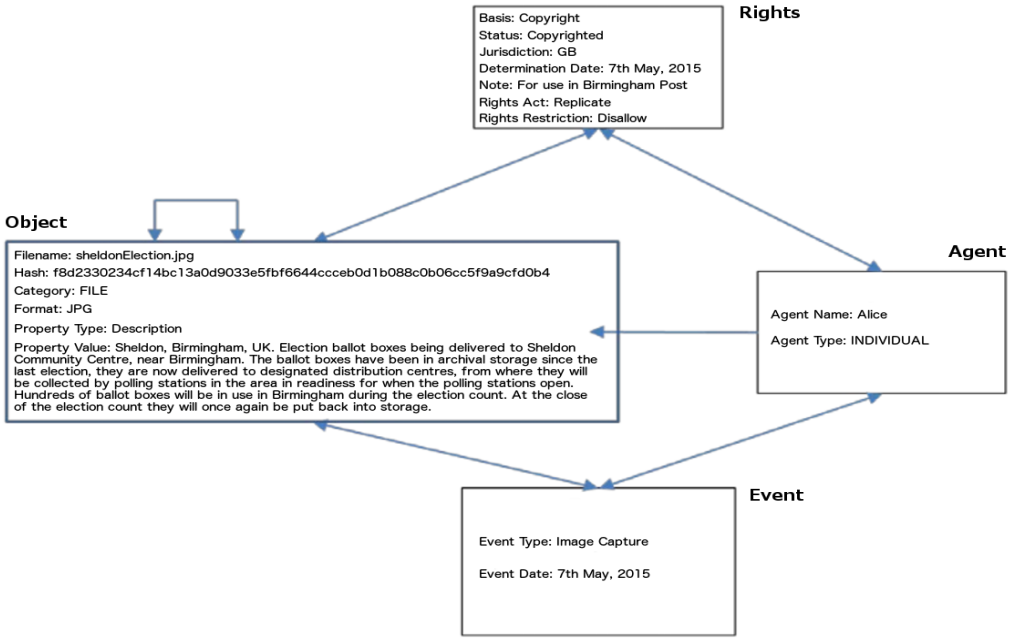


Figure 8.10: A PREMIS record of Alice's Picture of the Sheldon Election Ballot Boxes [12]

Figure 8.11 shows Alice using Provenator to store her PREMIS record of the Sheldon ballot box picture. It shows Alice using MetaMask to confirm her digital signature required for the necessary blockchain transactions.

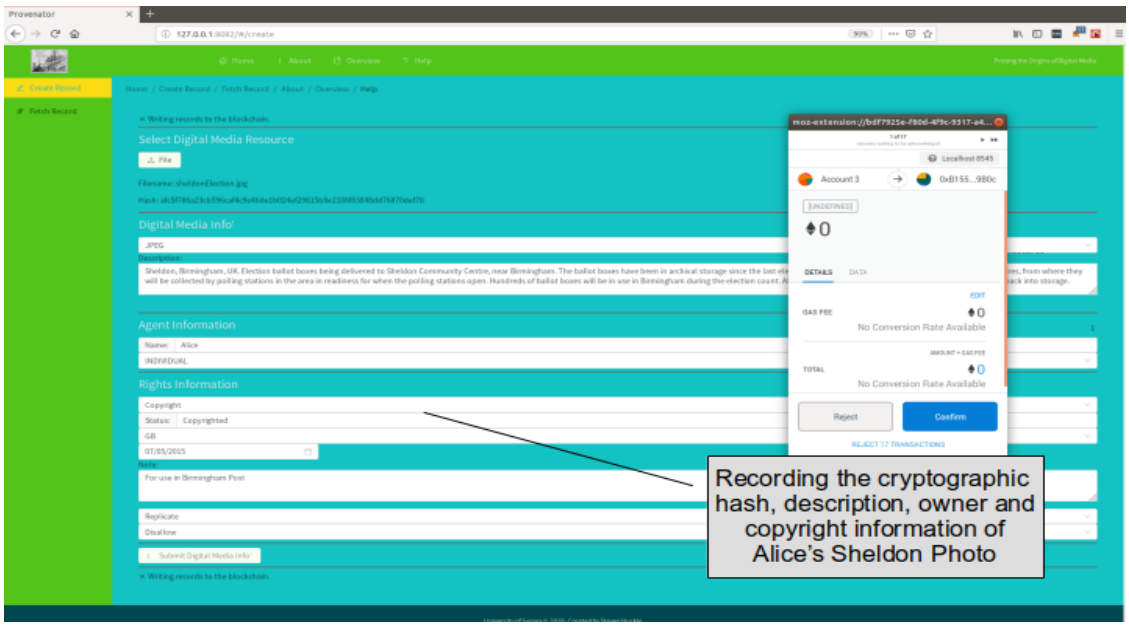


Figure 8.11: Alice Using Provenator to Create a Blockchain-based PREMIS Record of Her Picture of the Sheldon Election Ballot Boxes

Finally, Figure 8.12, below, shows the final scenario imagined in *Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains* [12]. There, an Editor of the New York Times loads Alice's picture into Provenator. That generates a cryptographic hash of the picture, whereby, because Provenator was used to record the PREMIS metadata of the picture, the Editor can retrieve that data. Moreover, due to the deterministic and collision resistance properties of cryptographic hashes, the paper is confident that the records match that same image [12].

Furthermore, because Alice used MetaMask to add her digital signature to the blockchain transactions creating that data, the paper is confident that Alice is the originator of that record. Hence, rather than going to great investigative lengths to prove the origins of Alice's image, the New York Times would have been able to check the validity of the picture only by uploading it to Provenator.

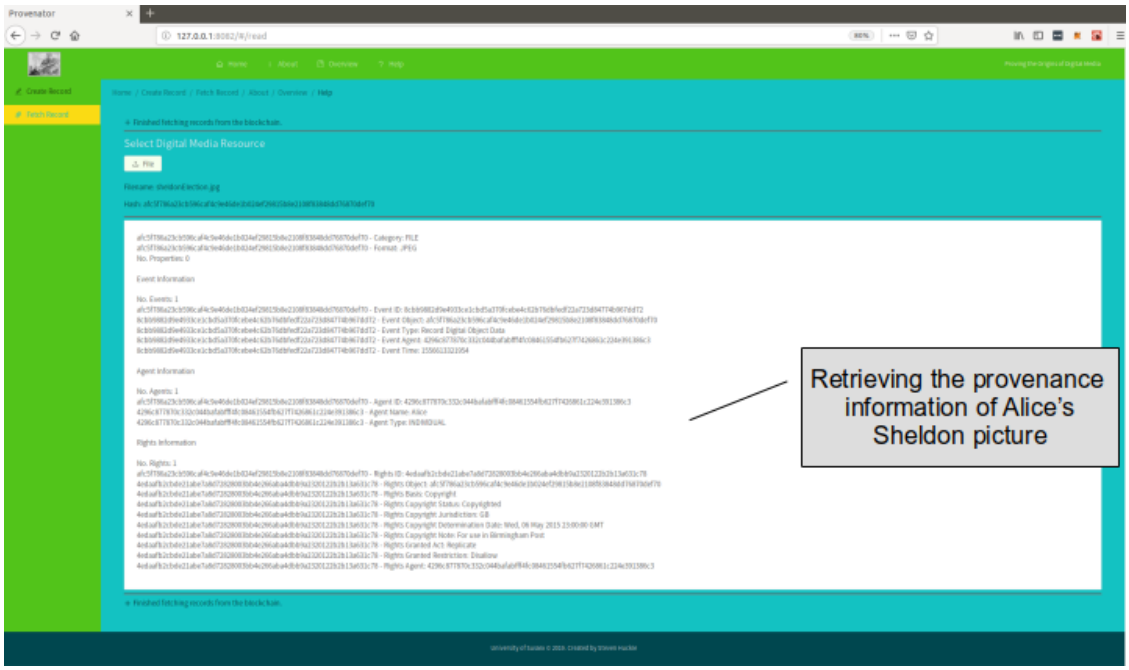


Figure 8.12: The New York Times retrieving the blockchain record of the picture of the Sheldon Election Ballot Boxes

8.3 Analysis

This analysis section constitutes the *evaluation* and *conclusion* stages from DSR. The third of the subordinate questions of the research objective asks whether blockchains can help counter fake news. The DSR artefact Provenator, described above through examples, suggests the answer must be yes. Indeed, Figures 6.6 through 6.11 show that blockchains allow content creators to establish the ownership of the digital media they create, so they can mitigate the risks of online piracy and the misuse of media to propagate fake news [216].

In a 2009 paper, Cheney et al. argue that provenance is an essential measure for ensuring the integrity of all digital infrastructures because it helps ensure properties of repeatability, integrity and authenticity, thus making it easier to, "detect and prevent failures, analyse errors, and discourage malfeasance by increasing transparency and accountability" [23]. Thus, Cheney et al. believed that, by ensuring the trustworthiness of data, provenance would play an essential role in the ongoing digital revolution. That would not come without significant barriers, because "High-performance computing, formal verification, and security are widely appreciated to be challenging". However, blockchains have emerged since the publication of the paper by Cheney et al., and this thesis has shown, through the DSR artefact Provenator, that they offer innovative solutions to some of those challenges.

The PREMIS model of the DSR artefact Provenator allows Provenator to share the data it stores with other users and applications [226], a capability that increases copyright trust and transparency [227]. Furthermore, Provenator can store metadata about any digital media for which it can generate a cryptographic hash. Hence, the application has appeal above and beyond the digital images shown in the examples, above. For instance, the author's paper that formed the basis for this research - *Internet of Things, Blockchain and Shared Economy Applications* [1], describes using blockchains for rights management of digital audio. That tells the story of Imogen Heap, who released her song, *Tiny Human*, on a prototype music

platform that used blockchain technology to detail under what terms people could download her music [228].

However, as discussed in the author's paper that introduced Provenator, *Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains* [12], a strength of the application is also a weakness. The strength lies in the properties of cryptographic hashes, whereby the same digital media resource always generates the same hash. However, therein lies the weakness because changing a single pixel in that digital resource generates an entirely different cryptographic hash. Therefore, any malicious actor, wishing to claim the media for themselves, could easily defeat Provenator by merely changing a single bit. The paper also proposes that technologies such as perceptual hashing might overcome such a weakness [229], a proposal that is discussed in greater detail in the conclusion, which considers future iterations of Provenator.

Since the publication of *Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains* [12], the idea of using blockchains for copyrighting purposes has gained further traction. Shang et al. quote this author directly when using blockchains to identify fakes by tracking news [230], and on the 9th of January 2018, camera manufacturer Kodak announced KODAKOne, which the company described as a revolutionary new image rights management blockchain-based platform[47]. Although at the time of its announcement in 2018, KODAKOne was limited to images, the platform Kodak described was to have capabilities above and beyond Provenator. For example, it would allow content creators to upload their pictures, create a blockchain-based license for each, and use a KODAKOne cryptocurrency to buy and sell provably rights-cleared and protected digital assets. Furthermore, rights owners would be able to use web-crawling software to scour the internet looking for copyright violations [231].

The success of KODAKOne remains unclear. New platforms, such as that, are difficult to launch because they have the same network externalities of Enervator [216]. Take Provenator as an example; without the presence of a

[47]the Kodak blockchain initiative is described at https://www.kodakone.com/

considerable amount of records within the application's PREMIS architecture, it is difficult to expect a substantial number of people (let alone organisations such as The New York Times, who feature in Figure 8.11), to use the platform to retrieve copyright information. Quite simply, Provenator will only really be useful if it achieves wide-scale adoption. However, there are many successful examples of mass adoption of new technology, so such success is not without hope.

8.4 Summary

The research objective of this thesis asks whether blockchains can help humanity. This chapter focuses on the third of four subordinate questions that help answer that overarching objective. It asks whether blockchains can help counter fake news, a question that is examined through the lens of the DSR artefact Provenator, a blockchain-based application that implements the PREMIS standard as a means of proving the provenance of digital media.

The answer to that third question is grounded in the author's paper *Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains* [12], which discusses a photograph that a supporter of Donald Trump alleged showed his opponents rigging votes. The New York Times went to great lengths to prove the picture was fake [223], but *Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains* proposed an innovative blockchain solution, Provenator, which is an application that is able to to quickly and easily establish the origins of digital media. The article creates a scenario that proposes the provenance mechanisms of Provenator could have saved the New York Times much bother. It is a scenario that is repeated above, too.

The proposed solution offered by Provenator is examined through the DT stages of *principles of form and function*, which describes the design of the application, and *expository instantiation*, which shows examples of how the artefact proves the origins of digital media. Finally, this chapter uses the DSR stages of *evaluation* and *conclusion* to analyse the proposal, which suggests that digital provenance, via Provenator, has the potential to help

fight fake news. However, similar to the DSR artefact Enervator, the cryptocurrency that incentivises energy efficiency and which is described in Chapter 6, that relies on network externalities and the application's wide-scale adoption.

9 Blockchains and Humanitarian Aid

This thesis develops four questions that help answer the research objective as to whether blockchains can help humanity. The fourth of those questions asks if blockchains can address criticisms of humanitarian aid.

This chapter examines that fourth question. It does so by introducing the design science research (DSR) artefact ReportAid, which is a blockchain-based application that implements the International Aid Transparency Initiative (IATI) for increasing the transparency of reporting humanitarian financing[48]. The main idea of ReportAid is to use blockchains to document humanitarian aid, thereby adding the quality of *trust* to transparent aid reporting.

First, this chapter provides some background to ReportAid. Then, it describes the design of ReportAid and discusses that artefact in an imagined scenario where it is used to document the European Commission's 2015 response to the Ebola crisis in West Africa. The chapter ends with an analysis of that scenario.

9.1 Background

The novel idea to use blockchains in the humanitarian aid sector came as a result of a University of Sussex Masters Student, studying within the university's Science Policy Research Unit (SPRU). She wanted to enter SPRU's 2018 Science, Technology and Innovation Policy Challenge[49], and she intended to explore the cryptocurrency capabilities of blockchains as a novel means of providing finance during a humanitarian crisis. Back then, it was not something this author thought viable. Instead, after reading the *Grand Bargain* (GB) made at the 2016 World Health Summit (WHS), which committed to enhancing the transparency of mutual aid reporting [181], the author could see the immediate benefit of using blockchains as a means of delivering humanitarian aid reporting. Given his doubts, the author was

[48]The IATI standard is described at https://iatistandard.org/en/

[49]The 2018 Science, Technology and Innovation Policy Challenge is described at http://www.sussex.ac.uk/spru/newsandevents/2018/awards/sti-challenge

not part of the SPRU team that entered that 2018 Policy Challenge. He did, however, develop his idea for aid reporting - ReportAid is the result of that.

9.2 The Design of ReportAid

This section constitutes the design theory (DT) steps of *principles of form and function* and *expository instantiation* since it outlines the blueprint for ReportAid and shows numerous screenshots of the artefact in use.

ReportAid is a blockchain-based application for humanitarian aid reporting. It is open-source commons-based peer production software that exists on the source code repository GitHub[50]. Figure 9.1 shows a screenshot of the homepage of that repository.

Figure 9.1: ReportAid on GitHub

[50]ReportAid is available at https://github.com/glowkeeper/ReportAid

The GB adopted the International Aid Transparency Initiative (IATI) as the United Nation's standard open-data format for documenting aid finance [182]. The IATI is an open data standard that defines specific entities that need recording. Figure 9.2, below, shows ReportAid is a blockchain-based application that allows users to input, amend, and read IATA standard organisation and activity records. Hence, ReportAid represents an implementation of the Financial Tracking Service (FTS) of the U.N. Office for the Coordination of Humanitarian Affairs (OCHA) (The FTS is described in more detail in Chapter 4.

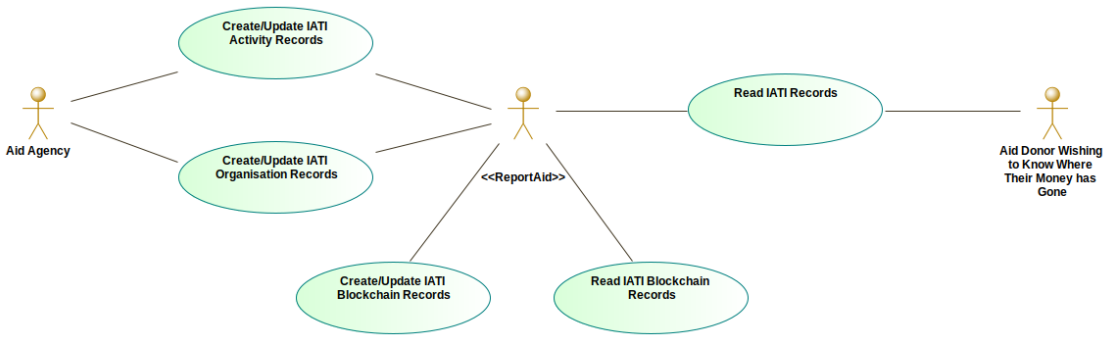


Figure 9.2: A Use Case Diagram for ReportAid

9.2.1 Principles of Form and Function

Figure 9.3, below, shows the ReportAid smart contract implementation of the IATI organisations standard. That is used to describe planned future budget information for aid funding[51]. Described is a top-level IATIOrganisations element (this contains information such as the generation date of the report), which has at least one IATIOrganisation element (containing the report's language and currency type). That IATIOrganisation element links to other information describing the aid, such as the reporting organisation, associated country budgets and any supporting documentation.

[51]The IATI organisation information that must be published is described at https://iatistandard.org/en/guidance/preparing-data/organisation-information/what-goes-on-your-organisation-file/

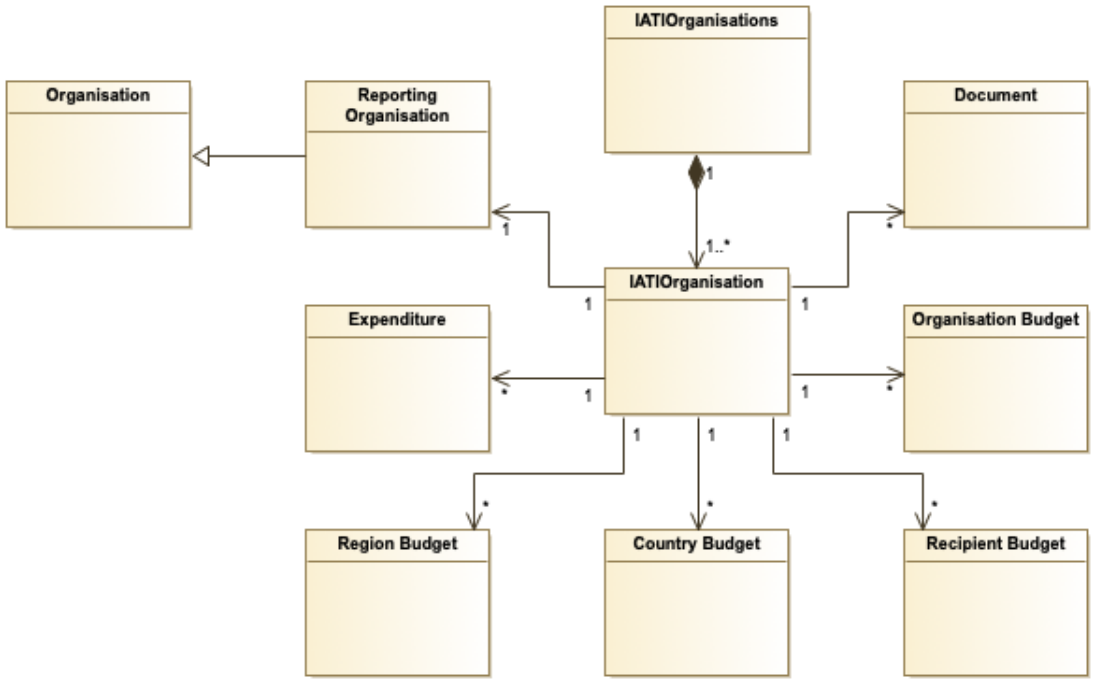


Figure 9.3: ReportAid IATI Organisations Smart Contracts

Figure 9.4, below, shows the ReportAid smart contract implementation of the IATI activities standard. A large number of fields describe IATI activities, and ReportAid, at the time of writing, has not implemented all of those; however, it does support all the mandatory fields, as well as one or two that are recommended[52]. Figure 9.4 shows a top-level IATIActivies element (which contains information such as the generation date of the report). That features at least one IATIActivity element (containing information such as the default currency type and the degree to which the activity relates to humanitarian aid), which links to information such as the organisation participating in the activity, the sector and territory to which the activity belongs, as well as budgetary data. A single reporting organisation produces an activity report.

[52]The IATI activity information that must be published is described at https://iatistandard.org/en/guidance/preparing-data/activity-information/activity-information-you-can-publish/

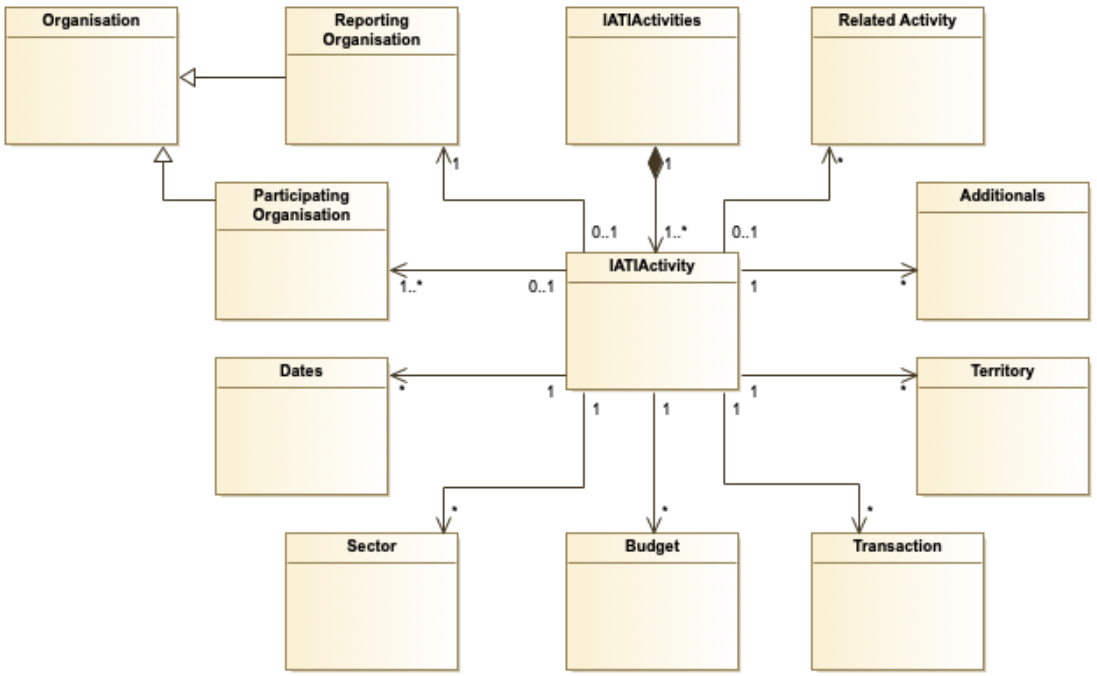


Figure 9.4: ReportAid IATI Activities Smart Contracts

Similar to the applications discussed previously in this thesis, ReportAid is a web-based application that depends on the web browser extension MetaMask.

At the time of writing, ReportAid includes 149 JavaScript and 42 Solidity source files, as well as 16 typescript definition files for its smart contract components. The application totals 22890 lines of code. Total development time was approximately a year. Porting IATI to the blockchain was the most time consuming of all the development effort since the standard is extensive and features complex relationships between its constituent parts - modelling that correctly, and representing it on the web interface, took a good deal of thought.

9.2.2 Expository Instantiation

Next, this chapter employs *expository instantiation* from DT when explaining the design of ReportAid by way of an example [187]. The scenario below starts the examination of whether blockchains can address criticisms of humanitarian aid.

The baseline report of the IASC GB transparency workstream cites the recent Ebola crisis as an example of incomplete, inaccurate, inconsistent and often inaccessible information that impacted the humanitarian effort in the diseases' epicentre in West-Africa [183]. Indeed, the report says that the lack of an adequately planned response hindered attempts to alleviate the outbreak because, at the time, no donor, government or aid agency was able to gain an overarching overview of available resources. The suggestion is that, were all the Ebola humanitarian aid efforts documented using the IATI standard and published to the UN's FTS, organisations would have had a more accurate picture of what was needed, thus improving the effectiveness of their response.

Despite such shortcomings, many of the organisations that are already using IATI make information about their development contributions available through existing aid information portals; a widely-used example is an open-source platform called d-portal[53]. That includes several IATI activities related to the world's response to the Ebola outbreak in West Africa. Hence, it contains data that ReportAid can import, thereby demonstrating its suitability as a proof of concept for blockchain-based humanitarian aid reporting. One such activity documented on d-portal was that carried out by the European Commission's Directorate-General for International Cooperation and Development (DEVCO), titled "A West African Response to Ebola" (AWARE), with IATI activity identifier XI-IATI-EC_DEVCO-2014/37785/0. That had a planned start date of 15th December 2015 and planned end date of 27th November 2018. The outgoing commitments of the activity totalled US$39,957,400. Its overall objective was to mitigate the harmful effects of the outbreak of the disease. Additionally, it was to contribute to the recovery of the most affected countries. Its specific purpose was to increase awareness of the symptoms of the disease and strengthen the resilience of primary healthcare systems. Appendix D includes the XML describing AWARE.

Figure 9.5, below, shows ReportAid creating the organisation record for AWARE.

[53]d-portal is available at http://d-portal.org/

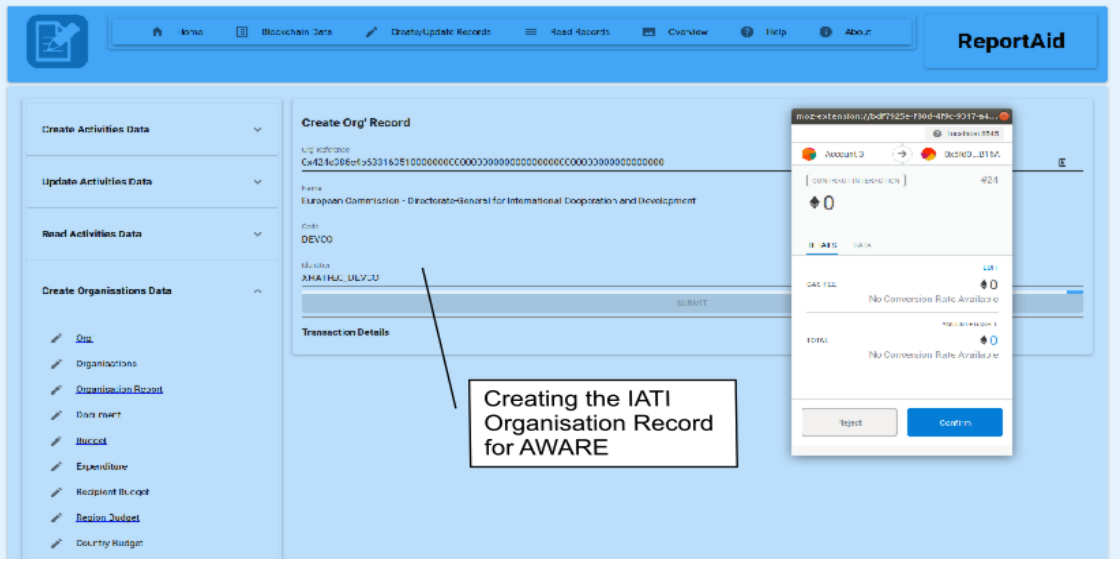


Figure 9.5: Creating the organisation record for DEVCO

The smart contract implementation of IATI Activities depends on a single top-level activities record. ReportAid must create that before it can record any specific activity. Figure 9.6, below, shows ReportAid using MetaMask to sign the transaction creating the necessary top-level activities record[54].

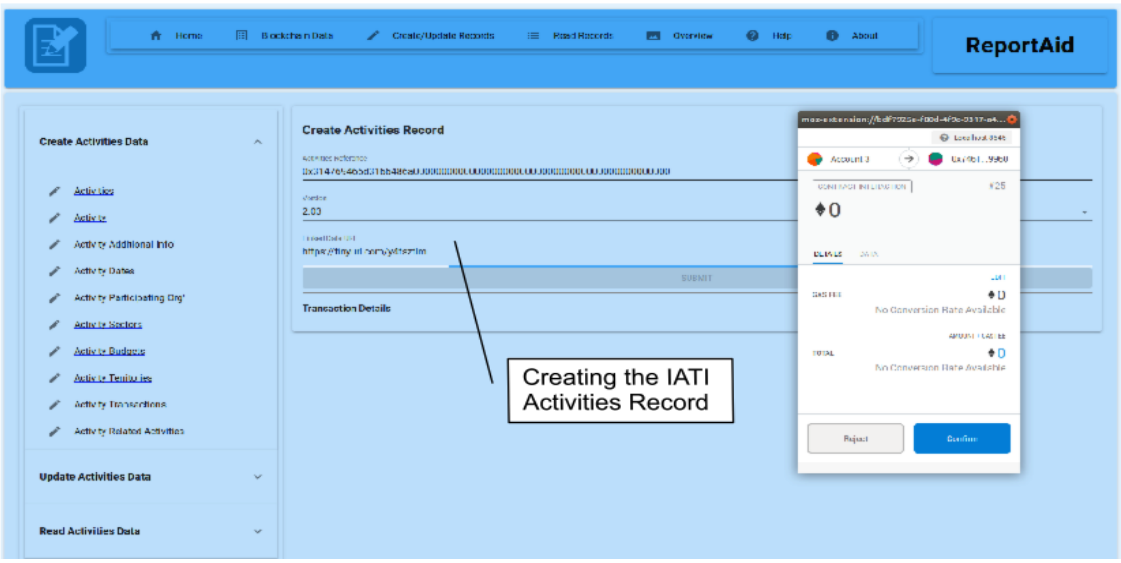


Figure 9.6: Creating the overarching activities record for the DEVCO Ebola activity

[54]At the time of writing, ReportAid requires the Linked Data URL to fit into a data type that is just 32 Bytes long (because that minimises the cost of storing such records on the Ethereum blockchain). Hence, all URLs need reducing to ensure they meet that requirement - The Linked Data URL shown in Figure 9.6, https://tinyurl.com/y4fsztlm, is a minimised URL representation of http://datastore.iatistandard.org/ns

Now the specific activity can be recorded. Figure 9.7, below, shows ReportAid signing the transaction creating the activity relating to AWARE.

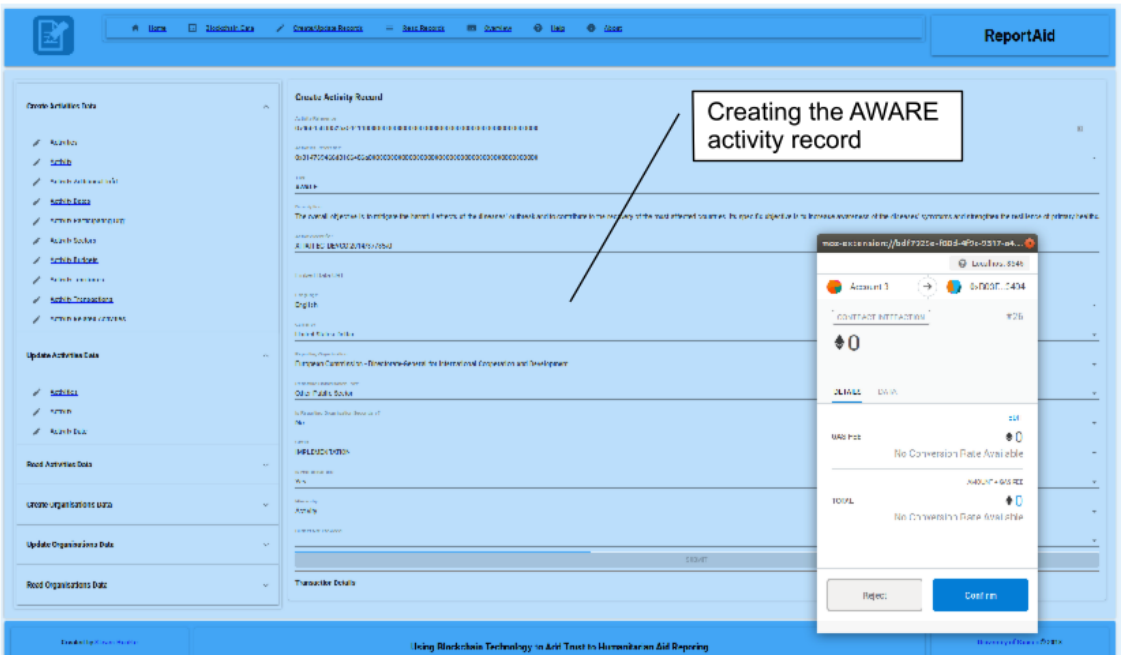


Figure 9.7: Creating the record for DEVCO's AWARE activity

Subsequently, anyone can read that activity record. Furthermore, that data can be trusted because the transaction that created that record was digitally signed. Figure 9.8, below, shows ReportAid retrieving the information created in Figure 9.7.

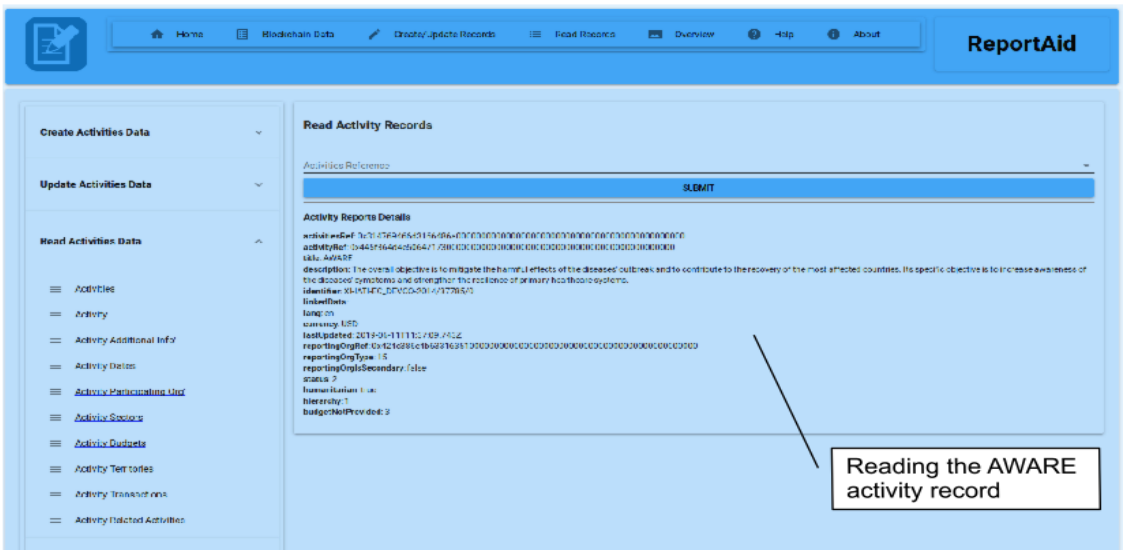


Figure 9.8: Reading the record for DEVCO's AWARE activity

The AWARE activity had a planned start date of 15th December 2015, an actual start date of 9th March 2015 and a planned end date of 27th November 2018. Figure 9.9, below, shows ReportAid recording the planned start date.

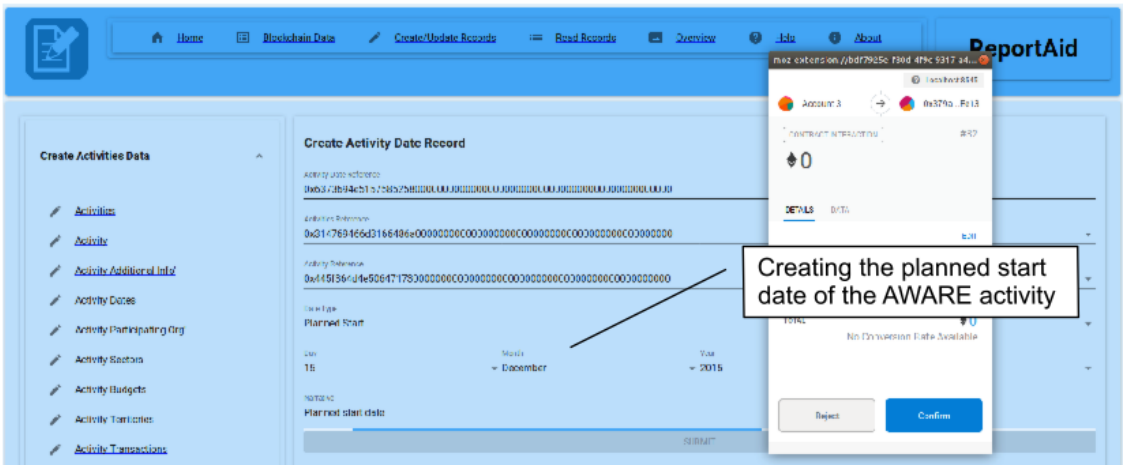


Figure 9.9: Creating the planned start date

Figure 9.10, below, shows ReportAid subsequently retrieving those dates.

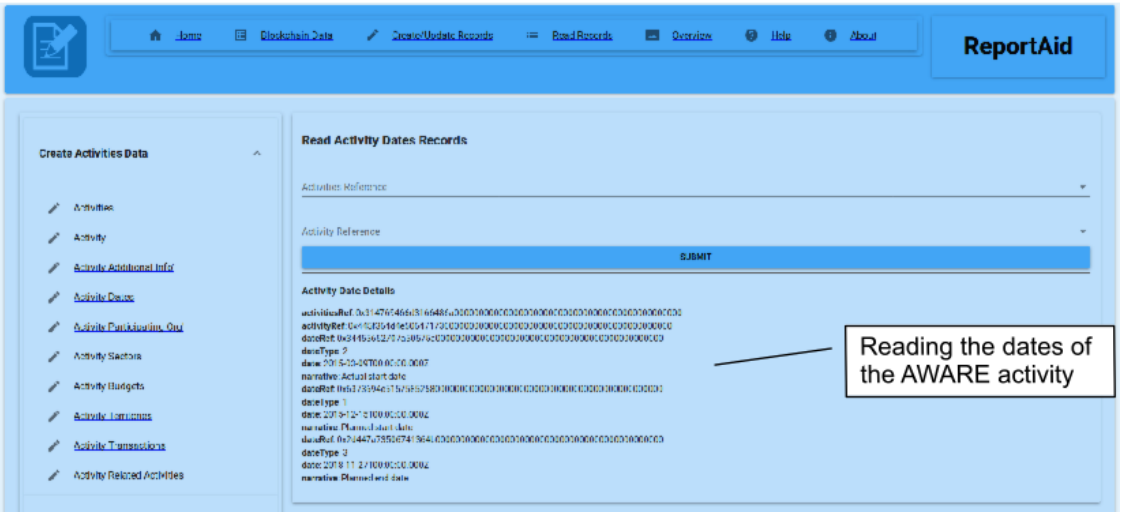


Figure 9.10: Retrieving the activity dates

Figure 9.11, below, shows ReportAid recording AWARE's budget commitment of US$28,000,000.

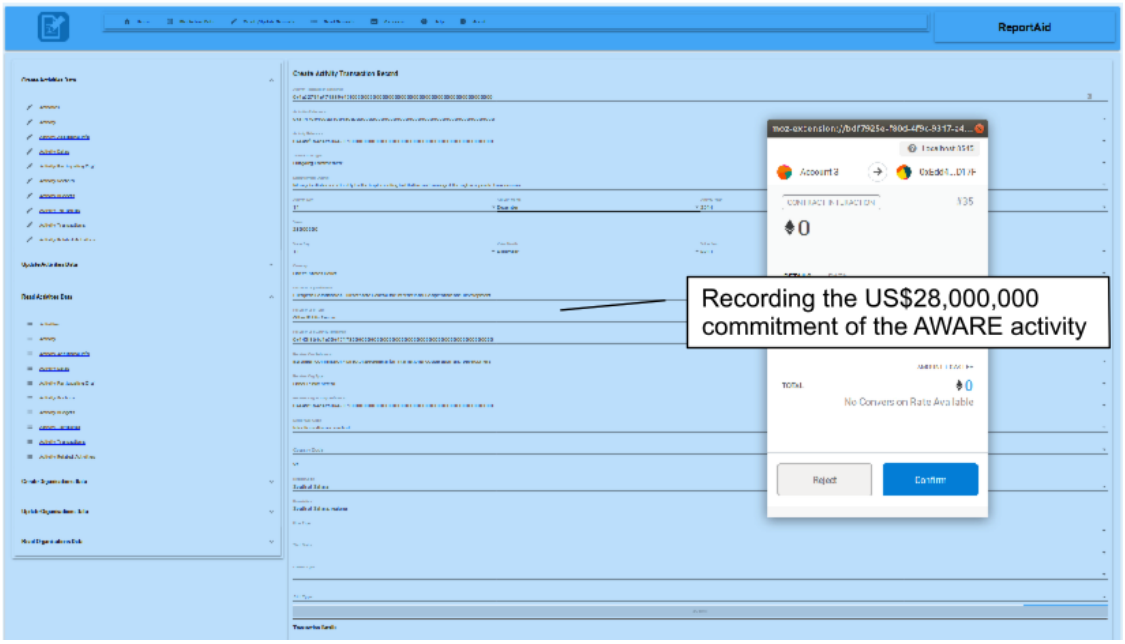


Figure 9.11: Creating the primary transaction record of DEVCO's AWARE activity

Figure 9.12, below, shows ReportAid subsequently retrieving that record.

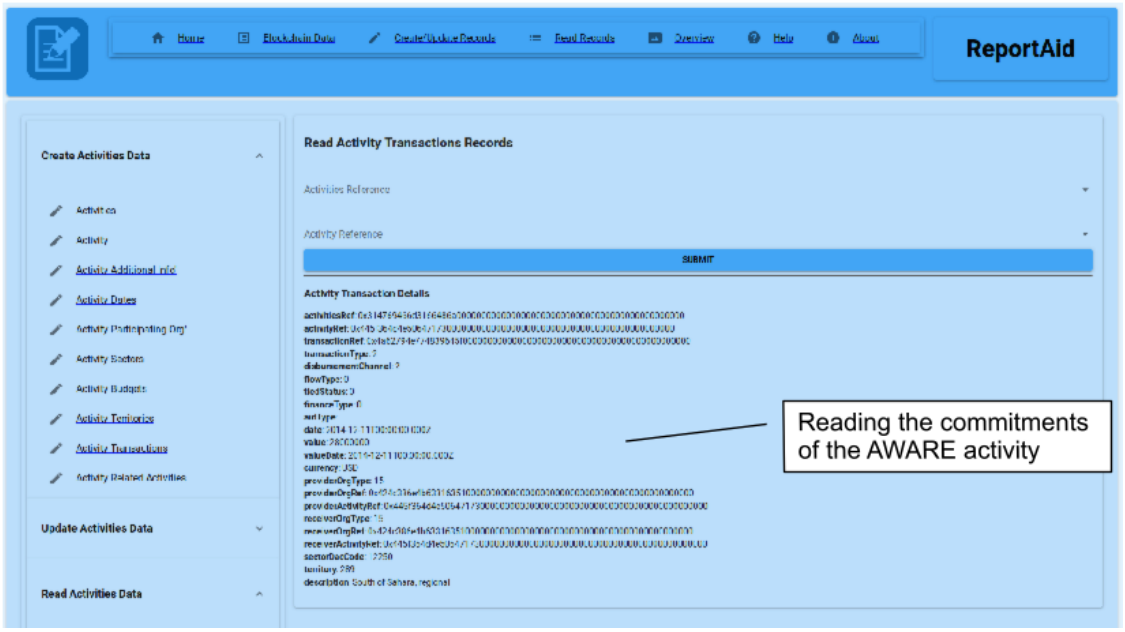


Figure 9.12: Reading the primary transaction record of DEVCO's AWARE activity

The AWARE activity recorded on d-portal contains more information, such as other budgetary disbursements, administrative contact information and links to other activities related to AWARE. At the time of writing, ReportAid

was able to model most of that data, however showing that here would add little to the discussion.

9.3 Analysis

This analysis section constitutes the *evaluation* and *conclusion* stages from DSR. This chapter focuses on whether blockchains can address criticisms of humanitarian aid. The DSR artefact ReportAid, which is shown above implementing the IATI standard whereby it can record the European Commission's 2015 response to the Ebola crisis in West Africa, suggests that the mechanisms of blockchains can help address such criticisms.

Coppi says, "Few advanced use cases of blockchain exist in the humanitarian sector. Instead, much discussion relates to potential and anticipated uses of the technology" [232]. ReportAid is a unique and advanced humanitarian use-case of blockchains that realises some of Coppi's supposed potential of the technology. However, there are several factors to consider beforehand. Those factors are discussed below.

Even before the Grand Bargain made at the 2016 World Health Summit (described in Chapter 4), the Inter-Agency Standing Committee, a forum that was founded by UN and non-UN humanitarian partners in 1992 to strengthen mutual assistance, had formed a Humanitarian Financing Task Team (HFTT)[55], tasked with researching financial transparency because they believed it helped fight corruption through providing the keys to understand, "why, how, what, and how much" [233]. The HFTT defined the *3Ts* of transparent reporting:

1. **Traceability**. The entire transaction chain of aid data must be traceable.
2. **Totality**. Financial information must be complete and relevant.
3. **Timeliness**. Aid information should be up-to-date [183].

The mechanisms of blockchains address those '3Ts' of transparent reporting. First, blockchains satisfy the traceability criteria because their records are publicly viewable and all transactions created are traceable

[55]More information about the work of HFTT is available at https://interagencystandingcommittee.org/humanitarian-financing-task-team

algorithmically [216]. Secondly, they meet the totality criteria because their records are practically impossible to change and the present state of the blockchain is a deterministic function of the genesis block and its ensuing transaction history [26]. In other words, a blockchain represents a historical record of all transactions ever recorded on its network. Thirdly, they fulfil the timeliness criteria because all records are timestamped. Therefore, anyone viewing the records can see just how timely they are.

However, might the HFTT have missed a 'T', namely, trust? Trust is the glue binding society together because it gives us confidence in situations that might otherwise harbour unknown risks [166]. Society does not necessarily achieve prosperity as the result of an abundance of natural resources or brilliance of intellect. Neither is that an inevitable result of systemic ideologies, such as frictionless free markets or the communitarian approach of commons-based peer production. Those things may have an important role to play, but ultimately, prosperity, in any form, comes as a result of "spontaneous sociability", achieved through trust because that is the crucial ingredient of any relationship and healthy relationships lead to success [14]. As was shown in Chapter 2, a blockchain's decentralised exchange mechanisms go above and beyond a traditional distributed database because they use public-key cryptography to create records, which means, unlike any database, they include a publicly auditable permission scheme. The result is that blockchains have capabilities that are suitable for determining integrity and authenticity because they represent a cryptographically secured immutable database technology. In other words, blockchains have inbuilt trust mechanisms [12]. Hence, ReportAid is an innovative example of an application for humanitarian aid reporting that, by using blockchains, adds that vital ingredient of trust. For example, when an aid organisation adds a record to its implementation of the IATI standard, users can trust it is that organisation that has created that record because they have digitally signed the transaction that did so.

However, there are significant barriers to the uptake of blockchains in the humanitarian sector.

1. **Technological**. Aid organisations using ReportAid would have to get used to new technology, whereas traditional databases have been around much longer and are, therefore, much better understood. There is likely to be pushback from IT departments too, because blockchains could, potentially, make them redundant.

2. **Organisational**. Public blockchains are inherently non-hierarchical, so they cannot be controlled by any single entity [12]. However, the FTS is a reporting platform run by OCHA. Hence, a fully-public blockchain-based system may challenge centralised, top-down governance and related assumptions the UN have about reporting on their aid funding.

3. **Cost**. Even though ReportAid is a working prototype of a blockchain-based implementation of IATI, were OCHA to invest in the technology, it may incur significant upfront costs, including those required for further development of the software, training users how to use it, and software maintenance. However, by replacing a traditional database architecture with a public blockchain, OCHA (and any organisation using the technology) may make significant long-term cost savings on infrastructure.

The WHS recognised that OCHA's FTS needed enhancing [184], and despite the barriers to uptake, this chapter proposes ReportAid, as a blockchain implementation of IATI that adds trust to the traceability of humanitarian aid reporting, might be that enhancement.

9.4 Summary

The research objective of this thesis asks whether blockchains can help humanity. This chapter focuses on the fourth of four subordinate questions that help answer that overarching objective. It asks whether blockchains can address criticisms of humanitarian aid, a question that is examined through the lens of the DSR artefact ReportAid, a blockchain-based application that implements the IATI standard for aid reporting. ReportAid is shown above documenting the European Commission's response to an Ebola outbreak in West Africa.

The proposed solution to that fourth question, offered by ReportAid, is examined through the DT stages of *principles of form and function*, which describes the design of the application, and *expository instantiation*, which shows examples of how the artefact uses the IATI standard to report on humanitarian aid. Finally, this chapter uses the DSR stages of *evaluation* and *conclusion* to analyse the proposal, which suggests that ReportAid, through its IATI reporting mechanisms, has the potential to help address criticisms of humanitarian reporting, because blockchains enable the *4Ts* of transparent aid reporting:

1. **Traceability**.
2. **Totality**.
3. **Timeliness**.
4. **Trustworthiness**.

However, this chapter also finds that there are significant technological, organisational and cost barriers that need overcoming before blockchain-based tools, such as ReportAid, are adopted by the humanitarian community.

10 Conclusion

This thesis asked the following research question:

Can blockchains help humanity?

That overarching question was the natural result of some of the author's previously published work, which asked whether blockchains can help address some contemporary problems:

1. Can blockchains help reduce energy consumption?
2. Can blockchains help digitise the informal sector?
3. Can blockchains help counter fake news?
4. Can blockchains help address criticisms of humanitarian aid?

Chapter 6 examines the first question, above, and whether blockchains can help reduce energy consumption. It describes the design science research (DSR) artefact Enervator (EOR), a unique cryptocurrency token that incentivises energy efficiency. It also describes the DSR artefact Eneradmin, which administers EOR. By showing examples of Eneradmin setting parameters so that the value of EOR changes with the decrease or increase of global per capita energy consumption and total primary energy supply (TPES), the chapter showed that blockchains can help address concerns about energy consumption. Indeed, the value mechanisms of Enervator may help increase 'total social welfare' [209], because the token's value will rise when both consumers and producers become more efficient, with the result that the environment benefits, too. Thus, EOR can help internalise some existential feelings of helplessness, and thereby, it may mitigate people's feelings of futility and that nothing can be done about the climate emergency. However, the success of a cryptocurrency like EOR relies on its wide-scale adoption.

Chapter 7 examines the second question, above, and whether blockchains can help digitise the informal sector. It describes Enerchanger, a DSR artefact for exchanging a sovereign currency for EOR. By showing examples of Enerchanger exchanging Indian Rupees for EOR, thereby exchanging physical cash for a digital equivalent, the chapter showed how

blockchains could help bring digital cash services to those who may have none. That brings other advantages, too. EOR removes the counterparty risk of traditional sovereign currencies and improves the visibility and availability of finance, thereby increasing the transparency of money transactions. That has positive implications for tackling financial fraud. However, such benefits rely on governmental support for cryptocurrencies, a move that many governments appear reluctant to make, perhaps due to concerns regarding monetary sovereignty.

Chapter 8 examines the third question, above, and whether blockchains can help counter fake news. It describes Provenator, a DSR artefact that records provenance metadata for digital media objects. By creating a scenario whereby Provenator was used to record the origins of an image that was used out of context to claim voting irregularities during the 2016 U.S. Presidential campaign, the chapter showed that blockchains could help counter online propaganda. They do so because they allow for copyright transparency. Furthermore, the PREMIS model of Provenator may allow the application to share the data it stores elsewhere. Provenator is also able to store metadata about any digital media, so it has uses beyond digital images. However, much like Enervator, the success of a tool such as Provenator relies on its wide-scale adoption.

Chapter 9 examines the fourth question, above, and whether blockchains can help address criticisms of humanitarian aid. It describes ReportAid, a DSR artefact for humanitarian aid reporting. By creating a scenario whereby ReportAid documents the European Commission's response to the Ebola outbreak in West Africa, the chapter showed that blockchains could indeed help address criticisms of humanitarian aid, because they enable the *4Ts* of transparent aid reporting, namely traceability, totality, timeliness and trustworthiness. However, there are significant technological, organisational, and cost barriers to overcome before a tool such as ReportAid is adopted for aid reporting.

By providing blockchain-based DSR artefacts that are proof of concepts that demonstrate solutions to the four questions used to examine the overarching research objective, this thesis concludes that blockchains can

help tackle a variety of challenges facing humanity. However, there are significant obstacles to overcome for that to be so. Furthermore, that could be a form of *techno-determinism*, a topic explored in greater detail below.

10.1 Implications

Chief amongst the implications of this thesis is the impact blockchains may have for regulators. The DSR artefacts included in this thesis demonstrate proof of concepts as to how blockchain technology offers extremely efficient and robust means for making trust easily accessible, due to its cryptographic mechanisms for establishing when, where, and by whom records were created. Indeed, the technology's cryptographic mechanisms can provide absolute verification of information, where, "for the first time in the history of humanity, there is the potential to create a permanent public record of who owns what, which no single or third party controls or underwrites, and where we can all reliably agree on the correctness of what is written" [166]. Hence, whereas society used to look up to trusted lawmakers and experts as oracles of truth, now it may be possible to look to blockchains, instead.

Additionally, were society to embrace the democratic ideals of commons-based peer production (CBPP) and the free software movement, it might be possible to make a cultural shift away from the industrial economy and production that is inherently centralised, monopolised and hierarchical [129]. After all, CBPP is creating socially egalitarian assets by commandeering the means of production, whereby the movement removes the price hurdle of the free market and makes goods freely available - theirs is a belief in the freedom to know rather than the freedom to own [109].

However, there is a critique of arguing for tech' as a driver for realising a more equitable society. That is a form of *techno-determinism*, which envisages technologies as a Utopia that empowers everyone, no matter what their privilege, race, wealth, status or class [16]. The general narrative is that technology is an apolitical problem-solving tool that can overcome the problems facing humanity. Does that translate into

egalitarian societies, featuring a pro-democratic mode of cultural and informational production that creates active producers, liberated from mass consumer culture? Perhaps not; unfortunately, the *technology-as-saviour* approach is a top-down narrative imposed on the poor by elite Western graduates, who suggest that the Internet provides a solution to all of humanity's problems [234]. Indeed, Freire argues that "More and more, the oppressors are using science and technology as unquestionably powerful instruments for their purpose: the maintenance of the oppressive order through manipulation and repression" [75]. Therefore, the people most likely to benefit from Internet-driven solutions are the wealthy - the very people who represent the inequality and crass commercialism at the heart of the systemic injustices of Capitalism [113]. In other words, techno-determinism is a form of neocolonial free-market elitism.

Kreiss et al. also cast doubt on the promise of CBPP, "we do not believe that networked information exchange necessarily levels the social playing field, or that networked modes of social action are replacing their industrial antecedents" [107]. They critique the supposed positive social and psychological outlook of the practice, which proponents suggest enables flexibility and distributes wealth and power, factors that are opposed to the supposed rigid, power-driven and psychologically damaging practices of the industrial era. However, Kreiss et al. question whether modern industrial bureaucracy is quite as evil as it is sometimes cast. To refute such claims, they appeal to the philosopher Mark Weber, whose work they describe as promoting the social value of bureaucracy [235]. That is because bureaucratic industrialisation processes helped overcome the lack of distinct social spheres in feudal life by establishing stable rule systems. Hence, it introduced many societal benefits that replaced "the whims of kings" and the irrationality of traditional forms of domination [236]. Furthermore, Kreiss et al. suggest the bureaucratic form is deeply embedded into many of the modern values of meritocracy, accountability and legal equality. They describe four benefits of bureaucracies:

1. They separate professional roles from private lives.
2. Legal systems ensure the equal treatment of everyone.

3. They are fair because system rules transcend and constrain the actions of individuals.
4. Their scale means bureaucracies are uniquely suited to serving particular functions enabling modern social life [107].

The first point focuses on the quality of personal lives, something to which CBPP practitioners often state as a *good* of their method because independent workers, unencumbered by bureaucracy, are more flexible, allowing them more freedom to mix travel and work [237]. However, that is a point of contention for Kreiss et al., who suggest that the blurring of the distinction between working and personal domains undermines individual autonomy [107]. Krogh and Hippel suggest that an individual's motivation for offering volunteer contributions to open source projects includes, "fun, enjoyment, reputation building, learning and the private use of software" [110] and that the only financial aspect involves the possibility of signalling their skills to prospective employers. However, Kreiss et al. maintain that CBPP goods are a product of the system in which they are embedded, and the economic processes of that system often leverage the goods produced [107]. Indeed, examples of that are numerous and can take various forms, such as adapting Free/Libre and Open Source Software (FLOSS) to suit a firm's needs [238] or co-opting the software in its entirety, thus acquiring it for the sole use of the firm [239]. Hence, Kreiss et al. disagree that peer production methods result in goods that are non-market, non-proprietary and represent the antithesis to those produced by hierarchical industrial bureaucracies [107]. Given their concerns, rather than transforming society and becoming an emblem of social change, by challenging the bureaucratic form, about which, they portray many benefits, Kreiss et al. posit that the practice of CBPP makes people's lives worse!

Meadows argues that the problem is malfunctioning hierarchies, not the architecture itself. After all, hierarchies predominate in natural systems, where they evolve from the bottom up, and their function is to support the success of the originating subsystem [240] — unfortunately, many of the hierarchies instituted by humankind feature top-down control. Indeed, growing inequality suggests that it is the bottom layers, the poor, who

support the top layers, thereby making the wealthy wealthier. Dafermos writes that hierarchy is the result of *bounded rationality*, whereby the size of specific control is finitely limited; therefore, the most rational means by which a growing organisation's operations can scale is by introducing more hierarchical layers [19]. Dunbar's number may play a role there[56], whereby, if an organisation has more than one hundred and fifty employees, it may well need to coordinate its operations hierarchically. However, as has been shown, evidence from CBPP projects suggests that it is not inevitable. For example, Drupal currently powers nearly 2% of all global websites[57], and more than 1.3 million people have registered some intention to get involved with the platform[58]. Given boundless rationality and Dunbar's number, the expectation must be that Drupal would feature endless levels of hierarchy, but that is not so. The reason as to why not may lie in modularity, whereby, instead of top-down stratification, "modular product design makes hierarchical organisation unnecessary by mitigating the need for active coordination" [19].

10.2 Future Work

The discussion above about CBPP could generate research that proceeds in a number of directions:

1. The software development processes of CBPP and whether that translates into fairer societies, as proposed by Rozas et al. [17]
2. Software innovation and the actions of multiple, diverse actors in distributed environments [243][244]
3. The motivation to contribute to CBPP development [110]
4. Governance and the management of FLOSS projects as an alternative to how industrial economies produce software

Much of that research could juxtapose CBPP against the arguments of Kreiss et al. who argue that the traditional hierarchical model of the

[56]Social anthropologist Robin Dunbar proposed that the size of our brains places a limit on the number of people with whom individuals can maintain a stable social relationship [241]. The commonly quoted *Dunbar's number* is 150 [242]

[57]Usage statistics and market share of Drupal - https://w3techs.com/technologies/details/cm-drupal/all/all, accessed on 8th February 2019

[58]Getting involved - https://www.drupal.org/getting-involved, accessed on 8th February 2019

industrial economy is a more productive means of managing software development [107]. A Postmodernist researcher could look at the power relations within Drupal [194], and whether Hacker Culture plays a part in explaining the mode of operation there. A feature of such culture is its disdain for bureaucracy and authority, whereby hackers reject Weber's *Iron Cage* [235], favouring, instead, autonomous individuality [19]. Indeed, there could be many factors at play in the governance structures of projects similar to Drupal, all of which could constitute some fascinating research.

The DSR artefacts discussed in this thesis are also ready for further inquiry. Up to the time of writing, their development has been the result of the author's efforts alone. That is, perhaps, unsurprising, since it is common in open source work for a single programmer to complete any one task [238], and each of the artefacts produced for this thesis was aimed at the single task of answering the research objective and whether blockchains can help humanity.

However, now those tools have proposed solutions to that research objective, it would be interesting to expand their development to a wider CBPP team. For example, ReportAid is ready to be exposed to the wider humanitarian community, in the hope that they may wish to develop it further. Figure 10.1, below, describes Howison and Crowston's theory of *Collaboration Through Open Superposition*, which explains how that development might proceed. At the centre is ReportAid's codebase. It shows the wider developer community to the left. They attract new developers by providing opportunities to discover ways of working. Those new developers, in turn, create ideas for improving the existing software. Figure 10.1 also shows the core team to the right; they consider the ideas for improving the code, thereby superimposing new layers that get integrated into the codebase. Thus, the process contributes to constructive feedback loops both within the core team and the wider developer community. The whole process benefits users because functionality improves [238].

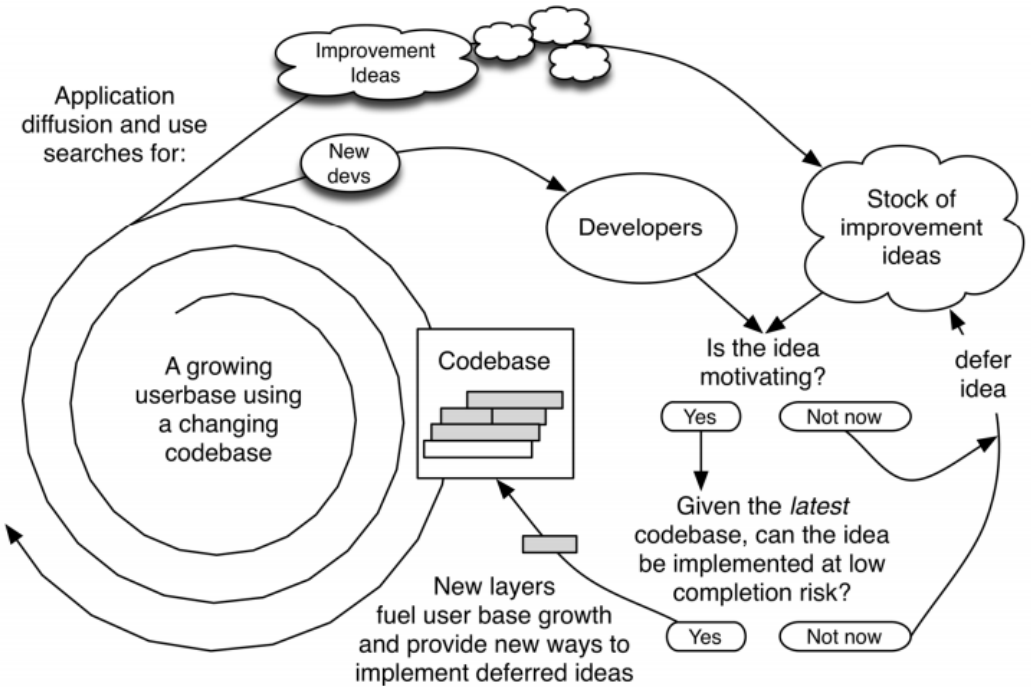


Figure 10.1: Howison and Crowston's theory - Collaboration Through Open Superposition

Below gives more consideration to the future possibilities and current limitations of the DSR artefacts featured in this thesis.

10.2.1 Enervator, Eneradmin and Enerchanger

EOR may represent an inherent contradiction. If, as proposed in the author's article for The Conversation [114], the CBPP practices of blockchains represent an opportunity to undermine the inequality of Capitalism (and its associated industrial carbon pollution), then even if EOR incentivises energy efficiency, it cannot offer a solution to those systemic failures if it supports the very mechanisms that have introduced such failures. Indeed, the author's paper, Socialism and the Blockchain [11] may offer an alternative approach. There, he explains that, instead of money, Marx envisaged a system of labour certificates, whereby people get rewarded according to the number of hours they spend in production. Those certificates could be used to buy all merchandise at cost price; goods whose value is determined in hours of labour [20]. Such certificates would not be allowed to circulate, so they could not be considered as capital

because Marx believed it was the money-commodity-money credit cycle that was core to Capitalist society [245]. That is because that cycle provides liquidity [246], and one of the foremost Economists of the 20th Century, John Maynard Keynes, thought liquidity as paramount to Capitalist economies because it made it possible to increase the means of production very quickly [247]. Socialism and the Blockchain proposes native digital assets that are used as Marxist labour certificates in support of a labour theory of value by matching the quantity of energy used in creating the asset with the amount of energy used by products over their lifetime [11]. Such certificates could be used to purchase products, but a smart contract would then remove them from circulation so they would not provide liquidity. If it is true that by introducing yet another means of liquidity, EOR helps prop up those same systems that are causing so much destruction, might labour certificates be more inline with a blockchain-based CBPP approach to climate change? However, although that could be a fascinating avenue in which to take further research, it might also represent unrealisable Utopian thinking. After all, society appears a long way from organising on Socialist principles; it is Capitalism that predominates. Hence, we should try and improve that system; the author contends that EOR might represent one small improvement.

Could EOR introduce unintended consequences? By internalising the problematic externalities of climate change, could there be negative psychological impacts? Might EOR generate some unwanted behaviour, such as not turning on the heating, even when the outside temperatures determine that the heating should go on. Such matters are only addressable through extensive testing of future iterations of Enervator.

Is the algorithm currently implemented by Enervator too simplistic? Could it offer better incentives? The author's article for The Conversation concluded that "if humankind is to avoid climate catastrophe, we need to take urgent action and find solutions that produce clean, sustainable energy" [114]. Enervator could incentivise clean energy, too. For example, if annual wind power grows, EOR's value increases. Future iterations could include such improvements.

Chapter 7 describes Enerchanger, where it proposes that EOR increases the visibility and availability of financial information. However, the cryptographic capabilities inherent in blockchain technology make it challenging to match transactions to real people [66]. That challenge is not insurmountable, especially if governments were to adopt their own cryptocurrencies, whereby they were in charge of issuing the necessary addresses for trading. That too is a field of study ripe for further research.

Finally, during a presentation for an Innovation forum discussing Energy Services Business Models, held by the UK Centre for Research into Energy Demand Solutions at The Fusebox, Brighton on October 4th 2019[59], this author discussed the barriers to uptake in front of Enervator. A slide showed the network externalities discussed in this thesis, whereby the hoped-for energy-efficient behaviour might only become apparent if the token managed wide-scale adoption. However, the person in charge of energy services at a UK county council had presented before the author, during which they explained they were seeking innovative solutions to lowering the council's consumption. The author offered Enervator as one such innovation. Could the solution to those network externalities come in the form of scaling back the goals of Enervator? Instead of incentivising global efficiencies, might it incentivise the energy consumption of that county council? The person in charge of the county council's energy services seemed to think so, and initial conversations about the idea appear promising.

10.2.2 Provenator

At the time of writing, the reports Provenator produces are somewhat limited. For example, it is not possible to search by the content owner. Additionally, the author can imagine Provenator working well on mobile, where he can see the benefit of being able to take a photograph or record some audio on a phone and immediately posting copyright data to the blockchain. Future iterations could include such enhancements.

[59]The presentation is available at https://github.com/glowkeeper/innovationForum

Chapter 8 and the author's paper *Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains* [12] discusses a weakness to Provenator, whereby any malicious actor can easily defeat the tool, simply by changing a single bit in a digital media object. However, that weakness is not insurmountable because there are technologies that are capable of noticing similarities between seemingly different digital objects. For example, Narwal et al. use fisher vectors and k-means clustering to classify comparable images [248]. Fisher vectors have been used to classify videos, too [249], so such technology appears to be an active area of computer vision research [250]. Another technology for recognising similar objects is perceptual hashing [229], which is used by organisations such as Shazam, Google and Youtube to detect copyright infringement [251]. Perceptual hashing works by calculating Hamming distances. Named after Richard Hamming, who introduced the concept in a 1950 paper on error detecting and error correcting codes [252], the general principle of the method is to establish the perceptual distance between two objects, *a* and *b*, which is the Hamming weight of *a minus b*. For example, the Hamming distance between *111000* and *111111* is three, whereas it is only one between *111001* and *111000*. Thus, perceptual hashing shows that the latter pair of binary numbers are more similar than the former. Hence, unlike cryptographic hashing, perceptual hashing is likely to show that a digital object featuring a single-bit change is likely to be the same as the original, a property that Provenator could employ to improve its matching capabilities.

However, the algorithmic complexity of the perceptual hashing solution, which is far more nuanced than the overview described above, is easily matched by the human eye, which is not so easily fooled by a single-pixel change [12]. The use case shown in Figure 10.2 hints that the ultimate arbiter of *fakeness* should be human, not technology. It shows that a forger has used a content creator's image out of context. To cover their tracks, the forger has introduced slight changes to the original. Unfortunately for them, the content creator has seen the image on the Internet, and although Provenator generates a different hash for that content, the content creator has the original image, so they can generate the hash from that and

retrieve the associated record from the blockchain. That shows their ownership and proves copyright infringement.

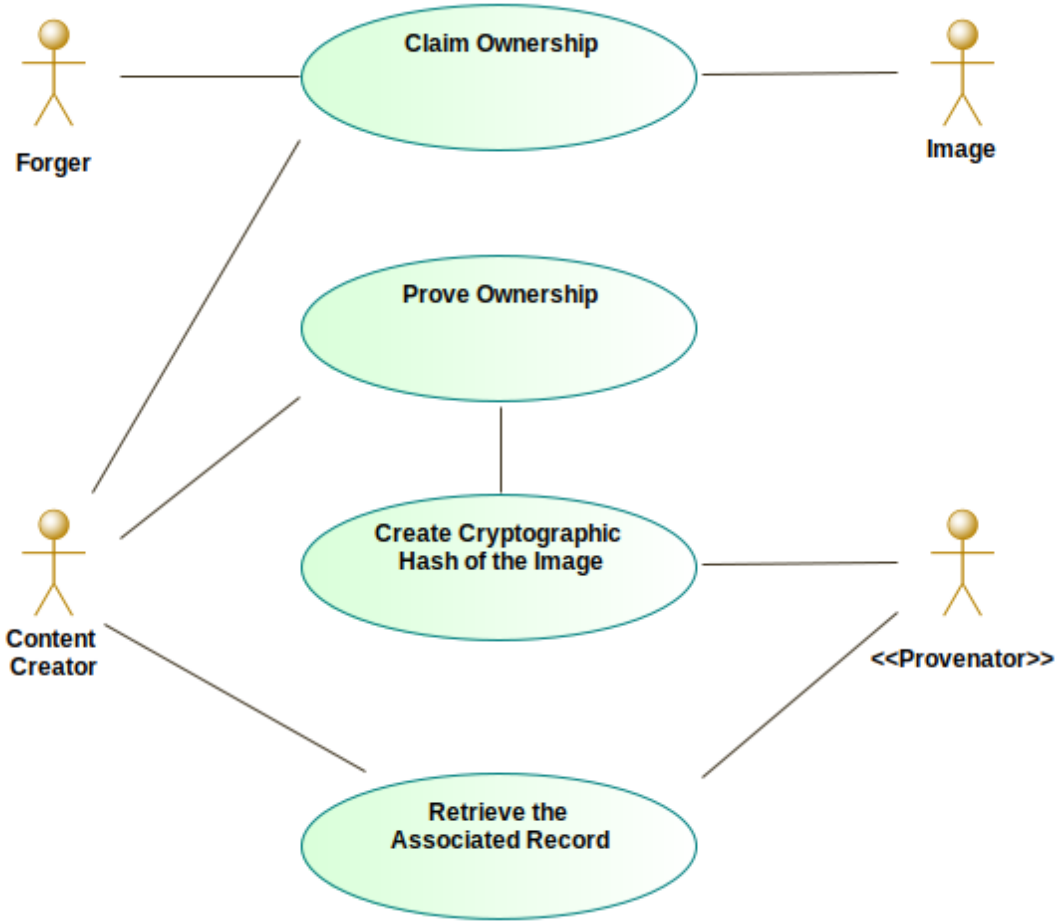


Figure 10.2: Proving the Identity of an Image Where a Single Bit has been Changed

10.2.3 ReportAid

At the time of writing, a staff member at Development Initiatives, the United Nation's UK-based IATI developer, has been evaluating ReportAid. It would be fantastic if Development Initiatives report back positively on blockchain's capability to add trust to humanitarian aid reporting and then the University of Sussex and they form a research partnership.

The current iteration of ReportAid is prototype software, so it is limited in several regards and therefore, future iterations of the application should address those limitations. For example, ReportAid only displays the very

latest records for a particular organisation or activity. However, all iterations of that record exist on the blockchain so the application could display those. Additionally, the reporting function of ReportAid currently outputs text records to the screen. A future release of the application should also output XML that conforms to the IATI standard.

However, does humanitarian aid have any place in a study that highlights the injustices of Capitalism and which hopes humanity moves on to a more socially egalitarian *commons* model? Freire argues that aid donors run the risk of their gifts becoming as odorous as the original act of oppression because they help maintain the unjust order that caused the need for aid in the first place; in other words, *humanitarian* generosity is itself a tool of the oppressor. Indeed, Duffield writes that the growth of non-state (charitable) intervention has enfeebled and enslaved weaker states because there is a link between aid, privatisation and globalisation [253]. Instead of humanitarianism, Friere suggests that it is only possible to transform into a more just society through *humanist* generosity [75]. Hence, rather than humanitarian programs that focus on giving aid *to* the people, might we achieve more sustainable transformation through programs that work *with* the people? Might progress be better engendered from within, through state education programs that focus on affirming longer-term human freedoms, rather than without, via perpetual privatised charitable aid focused on short-term needs? Such research might be outside the scope of work following this thesis, which primarily focuses on the role of technology to meet some of the challenges facing humanity. Still, it is an interesting conversation that could continue within further research.

10.3 Contributions to Knowledge

The five DSR artefacts created for this work make the following contributions to knowledge:

1. Enervator, Eneradmin and Enerchanger show how it is possible to create a cryptocurrency that incentivises energy efficiency.

2. The chapter describing Enerchanger creates a unique scenario by showing how the Indian Government could have used Enervator to help their demonetisation process and thereby fight financial fraud.

3. Provenator is a unique blockchain implementation of Preservation Metadata: Implementation Strategies (PREMIS), the open standard the application uses to create provenance metadata to verify the authorship and rights of digital media.

4. The chapter describing Provenator shows how blockchains could be used to fight fake news.

5. ReportAid is a blockchain-based humanitarian aid reporting application, which is a novel blockchain-based implementation of the International Aid Transparency Initiative (IATI), an open data standard for reporting humanitarian financing. That IATI implementation on the blockchain is also novel.

6. The chapter describing ReportAid shows how blockchains could help address criticisms of humanitarian financing.

10.3.1 Published Academic Articles

The basis of this thesis is four published articles, which also contribute to knowledge:

1. Steve Huckle, Rituparna Bhattacharya, Martin White and Natalia Beloff. Internet of Things, Blockchain and Shared Economy Applications. Procedia Computer Science. Volume 98, 2016, Pages 461-466. September 2016. https://doi.org/10.1016/j.procs.2016.09.074

2. Steve Huckle and Martin White. Socialism and the Blockchain. Future Internet 2016, 8(4), 49. 18th October 2016. https://doi.org/10.3390/fi8040049

3. Steve Huckle, Rituparna Bhattacharya and Martin White. Towards a post-cash society: An application to convert fiat money into a

cryptocurrency. First Monday. Volume 22, Number 3. 6th March 2017. https://doi.org/10.5210/fm.v22i3.7410

4. Steve Huckle and Martin White. Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains. Big Data. Volume 5, Issue 4. 1st December 2017. http://doi.org/10.1089/big.2017.0071

10.4 Reflections On the Research Methodology

It may have been possible to use a quantitative methodology for this thesis. For example, a sample set of users might have been given Enervator, and their behaviour measured. That way, it would have been possible to quantify the degree to which the token engenders any energy-efficient actions. Indeed, should discussions with the UK county council interested in using Enervator proceed favourably, a quantifiable approach to any further research could work well.

Since this thesis includes aspects of social science, the author also considered using Action Research (AR), which, in general, seeks transformative change through the simultaneous process of taking action and doing research, followed by a period of critical reflection. Kurt Lewin, then a professor at MIT, introduced AR in a 1946 paper, where he describes the methodology as a "comparative research on the conditions and effects of various forms of social action and research leading to social action", which uses "a spiral of steps, each of which is composed of a circle of planning, action and fact-finding about the result of the action" [254]. Such an approach may well have been useful for examining whether blockchains can help society through the deployment of several tools that are, essentially, social enablers. In particular, this thesis may have used a form of Action Research called *participatory action research* (PAR). Paulo Freire's *critical pedagogy*, and its expression as a tool for intervention, development and change within communities [75], heavily influences PAR, so it may have been an appropriate tool to deploy here as Friere has had an impact on the outcomes of this work.

However, the author is a Software Developer who builds applications, so he decided upon DSR because of its synthesis with design theory (DT) [186]. That enables a prescriptive approach to creating artefacts. For, example, the DT component of *principles of implementation* allows the developer to detail their design decisions, and the component of *principles of form and function* shows implementations of that design, which feeds into the latter stages of DSR, allowing an analysis of those implementations. Ultimately, the author is also interested in the social implications of technology and the tools he develops, and this thesis reflects that interest. Therefore, a methodology whose purpose is to acquire knowledge through creating artefacts fits well with both the author's interests and his skill set.

10.5 Summary

This thesis used design science research to examine the research objective:

> *Can blockchains help humanity?*

Four further questions examine that overarching question:

1. Can blockchains help reduce energy consumption?
2. Can blockchains help digitise the informal sector?
3. Can blockchains help counter fake news?
4. Can blockchains help address criticisms of humanitarian aid?

Five design science research artefacts helped examine those questions. Enervator is a unique cryptocurrency token that incentivises energy efficiency and helps reduce energy consumption. It is supported by Eneradmin, which can set the parameters that establish the token's value. Enerchanger simulates exchanging a sovereign currency for EOR, whereby it helps digitise the informal sector. Provenator is an application for creating provenance metadata for digital media. Therefore, it can establish the origins of content used out of context, thereby helping to counter fake news. Finally, ReportAid is blockchain-based software for humanitarian aid reporting that helps address criticisms of humanitarian aid. By answering those subordinate questions via those design science research artefacts, this thesis finds that blockchains can help humanity. However, there

remain significant technical obstacles to overcome. Nevertheless, this thesis has implications for regulators because it shows how society may be able to use blockchains as the ultimate oracles of truth.

A recent report for Oxfam calls for a dramatic transformation of the world's economies so that the burgeoning wealth gap is reduced [255]. Oxfam describes the systemic inequality of Capitalist society, "our economy is broken, with hundreds of millions of people living in extreme poverty while huge rewards go to those at the very top". The figures behind that claim are stark; in the year up to January 2019, the wealth of the world's billionaires increased by US$2.5 billion per day, totalling $900 billion. Meanwhile, 3.4 billion people, which equates to approximately half the world's population, are living on less than $5.50 per day. The number of people living in extreme poverty (under US$1.90 per day) has fallen from 1.9 billion in 1990 to 804 million in 2011, but since then, the rate of poverty reduction has begun to slow [256]. Inequality exists between the sexes, too, with men owning more than fifty per cent of the wealth of women, mainly because those women do millions of unpaid hours caring for their families [255]. Poverty is on the rise in Sub-Saharan Africa and the many conflict regions around the world. The living standards of the bottom forty per cent of the world's population are declining [256]. So-called first-world countries are not immune to the rise in inequality. A recent U.N. report on poverty in the U.K., the world's fifth-largest economy and home to many areas of immense wealth, particularly in London because it is a centre for global finance, found that 14 million people, a fifth of the population, live in poverty [257]. Four million of those are more than fifty per cent below the poverty line. Consequently, in the past decade, 1.5 million U.K. citizens have become destitute, unable to afford essentials. Many have become homeless, and many more get their daily calorie intake via food banks.

Given the evidence of systemic inequality of Capitalism and its associated industrial carbon pollution, the suspicion is that, if humanity is to have a positive future, it must ditch that system. This thesis wonders if the change required is the flat, decentralised and egalitarian systems of CBPP and the digital commons movement. Conway's Law would suggest so since its

primary tenet is that organisations design systems based on their communication structures [13]. Therefore, if society wants to become mutually collaborative, we need systems built on mutual collaboration, such as the blockchain technologies discussed in this thesis. However, that belongs to the *technology-as-saviour* narrative, which may offer false hope. Technology, in general, and blockchains in particular, can *help* tackle some of the challenges facing humanity (such as those described in this thesis). However, they cannot offer solutions in their entirety. For example, blockchains are unable to verify the trustworthiness of facts that originate outside of the digital realm [216]. Indeed, the author's paper - *Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains* [12], posits that although Provenator is able to establish the copyright metadata of digital media used within fake stories, it is incapable of proving the authenticity of a fake news story as a whole. That takes human endeavour.

Furthermore, a reviewer of an early draft of the author's paper, Socialism and the Blockchain [11], argued that the paper relies on, "the fundamental assumption of a working Internet". In Internet-connected Western societies, that assumption may be valid, but there are people around the world who are unable to access the Worldwide Web. For example, at the time of writing, just 41.8 per cent of the Indian population were online [146]. The solutionism of the techno-determinists would suggest that the end goal for the disconnected must be to connect and integrate into the current economic system. Indeed, India's demonetisation process, discussed in Chapter 4, appears to be just such a drive. However, Scott argues humanity cannot rely on such solutions because, although technology may help some individuals, "it does little to empower the broader social majority who remain reliant on the existing systems" [113]. Indeed, technological infrastructure cannot merely code-away the problems that are inherent in human relations [258]. It is impossible to solve all of humanity's issues by diversifying technical operations; we need to change political, economic, and cultural goals, too [259]. Rather than imposing technology on the marginalised, a better approach is to require action on the ground to correct systemic failures through social solidarity

alternatives [113]. Indeed, Freire argues that positive changes can only become apparent through reflective action that enables cultural synthesis, unity, organisation, and cooperation with those that are suffering [75].

Such arguments have convinced the author that it is not necessarily the technology implementing CBPP that offers hope for humanity, but rather the *principles* CBPP represents. Indeed, a presentation the author gave during this research advocated for the humanism of CBPP. It concluded with a clarion call, repeated, below:

"My dear audience, if like me, you believe we solve the inequality by opposing traditional hierarchies, then, just as the #MeToo campaign has begun to undermine elitist patriarchy, I challenge you to refute established top-down power structures. Enough is enough! Go and create, participate and collaborate with your peers. Show that flat and cooperative is best, and Be the Change You Wish To See in the World".

The author hopes that future research comes from this thesis, and this chapter makes some suggestions in that regard. Indeed, the DSR artefacts are obvious candidates for further study - examples are the value mechanisms of Enervator and whether the token could be used to incentivise renewable energy. Or perhaps Enervator could measure and affect consumption on a smaller scale than it does at the time of writing. However, the author's primary hope lies with you, dear reader, whom he hopes realises that clarion call by reflecting and acting on the values of the *commons* espoused throughout this work.

11 References

[1] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, “Internet of Things, Blockchain and Shared Economy Applications,” *Procedia Computer Science*, vol. 98, pp. 461–466, 2016 [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1877050916322190. [Accessed: 20-Nov-2017]

[2] Investopedia, “Cryptocurrency,” *Investopedia*, 29-Jul-2013. [Online]. Available: https://www.investopedia.com/terms/c/cryptocurrency.asp. [Accessed: 20-Nov-2017]

[3] G. Anand and H. Kumar, “Narendra Modi Bans India’s Largest Currency Bills in Bid to Cut Corruption,” *The New York Times*, 08-Nov-2016 [Online]. Available: https://www.nytimes.com/2016/11/09/business/india-bans-largest-currency-bills-for-now-n-bid-to-cut-corruption.html. [Accessed: 16-Jan-2017]

[4] N. G. Mankiw, “Principles of Economics,” in *Brief principles of macroeconomics*, Seventh edition., Australia ; Stamford, CT: Cengage Learning, 2015, p. 220.

[5] Eris Industries, “Explainer | Smart Contracts,” *Eris Industries Documentation*, 2016 [Online]. Available: https://docs.erisindustries.com/explainers/smart_contracts/. [Accessed: 19-Mar-2016]

[6] Douglas Harper, “Online Etymology Dictionary - Sovereign,” 2001–2007. [Online]. Available: http://www.etymonline.com/index.php?term=sovereign. [Accessed: 18-Jan-2017]

[7] Y. Benkler, “From consumers to users: Shifting the deeper structures of regulation toward sustainable commons and user access,” *Federal Communications Law Journal; Washington*, vol. 52, no. 3, pp. 561–579, May 2000 [Online]. Available: https://search-proquest-com.ezproxy.sussex.ac.uk/docview/213212452/abstract/73E56EE80A234093PQ/1?accountid=14182. [Accessed: 08-Oct-2017]

[8] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008 [Online]. Available: https://bitcoin.org/bitcoin.pdf

[9] T. Bosch, “Sci-Fi Writer Bruce Sterling Explains the Intriguing New Concept of Design Fiction,” *Slate Magazine*, 02-Mar-2012. [Online]. Available: https://slate.com/technology/2012/03/bruce-sterling-on-design-fictions.html. [Accessed: 11-Nov-2019]

[10] S. J. Huckle, M. White, and R. Bhattacharya, “Towards a post-cash society: An application to convert fiat money into a cryptocurrency,” *First Monday*, vol. 22, no. 3, Feb. 2017 [Online]. Available: http://firstmonday.org/ojs/index.php/fm/article/view/7410. [Accessed: 22-Oct-2018]

[11] S. Huckle and M. White, “Socialism and the Blockchain,” *Future Internet*, vol. 8, no. 4, p. 49, Oct. 2016 [Online]. Available: http://www.mdpi.com/1999-5903/8/4/49. [Accessed: 04-Oct-2017]

[12] S. Huckle and M. White, “Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains,” *Big Data*, vol. 5, no. 4, pp. 356–371, Dec. 2017 [Online]. Available: http://online.liebertpub.com/doi/10.1089/big.2017.0071. [Accessed: 19-Dec-2017]

[13] M. E. Conway, “How do committees invent?” F. D. Thompson Publications, Inc, Apr-1968 [Online]. Available: http://www.melconway.com/Home/pdf/committees.pdf. [Accessed: 09-Nov-2017]

[14] F. Fukuyama, *Trust: The social virtues and the creation of prosperity*. New York, NY: Penguin Books, 1996.

[15] M. Swan, *Blockchain: Blueprint for a New Economy*. O’Reilly, 2015.

[16] D. Rozas, A. Tenorio-Fornés, S. Díaz-Molina, and S. Hassan, “When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance,” Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3272329, Jul. 2018 [Online]. Available: https://papers.ssrn.com/abstract=3272329. [Accessed: 08-May-2019]

[17] D. Rozas, “Self-organisation in Commons-Based Peer Production,” p. 401, 2017.

[18] K. Crowston, K. Wei, J. Howison, and A. Wiggins, *Free/libre open source software development: What . . .* 2010.

[19] G. Dafermos, “Governance structures of free/open source software development examining the role of modular product design as a governance mechanism in the FreeBSD Project,” Next Generation Infrastructures Foundation, Delft, 2012.

[20] Pëtr Kropotkin, “Anarchism: Its Philosophy and Ideal | The Anarchist Library,” 1898 [Online]. Available: http://theanarchistlibrary.org/library/petr-kropotkin-anarchism-its-philosophy-and-ideal. [Accessed: 30-Jun-2016]

[21] The World Bank, “Concept of Informal Sector,” 2017. [Online]. Available: http://lnweb90.worldbank.org/eca/eca.nsf/Sectors/ECSPE/2E4EDE543787A0C085256A940073F4E4?OpenDocument. [Accessed: 19-Jan-2017]

[22] The Economist, “The Trust Machine,” *The Economist*, Oct. 2015 [Online]. Available: http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine. [Accessed: 17-Feb-2016]

[23] J. Cheney, S. Chong, N. Foster, M. Seltzer, and S. Vansummeren, “Provenance: A future history,” in *Proceeding of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications - OOPSLA ’09*, 2009, p. 957 [Online]. Available:

http://dl.acm.org/citation.cfm?doid=1639950.1640064. [Accessed: 25-Jun-2019]

[24] D. Rancic Moogk, “Minimum Viable Product and the Importance of Experimentation in Technology Startups,” *Technology Innovation Management Review*, vol. 2, no. 3, pp. 23–26, Mar. 2012 [Online]. Available: http://timreview.ca/article/535. [Accessed: 23-Apr-2019]

[25] V. Vaishnavi, B. Kuechler, and S. Petter, “Design Science Research in Information Systems,” 20-Jan-2004. [Online]. Available: http://www.desrist.org/design-research-in-information-systems/. [Accessed: 04-Apr-2019]

[26] Ethereum, “Sharding FAQs,” 06-Oct-2018. [Online]. Available: https://github.com/ethereum/wiki. [Accessed: 06-Oct-2018]

[27] F. Tschorsch and B. Scheuermann, “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies,” 464, 2015 [Online]. Available: http://eprint.iacr.org/2015/464. [Accessed: 28-Sep-2018]

[28] D. Chaum, “Blind Signatures for Untraceable Payments,” in *Advances in Cryptology*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. Boston, MA: Springer US, 1983, pp. 199–203 [Online]. Available: http://link.springer.com/10.1007/978-1-4757-0602-4_18. [Accessed: 28-Sep-2018]

[29] Andrew Poelstra, “On Stake and Consensus.” 22-Mar-2015 [Online]. Available: https://download.wpsoftware.net/bitcoin/pos.pdf. [Accessed: 09-Oct-2018]

[30] W. Dai, “B-money,” 1998. [Online]. Available: http://www.weidai.com/bmoney.txt. [Accessed: 28-Sep-2018]

[31] N. Szabo, “Unenumerated: Bit gold,” *Unenumerated*, 27-Dec-2008. [Online]. Available: https://unenumerated.blogspot.com/2005/12/bit-gold.html. [Accessed: 28-Sep-2018]

[32] A. Back, “Hashcash - A Denial of Service Counter-Measure,” Aug. 2002 [Online]. Available: http://www.hashcash.org/papers/hashcash.pdf. [Accessed: 12-Feb-2016]

[33] H. Finney, “RPOW - Reusable Proofs of Work,” 22-Dec-2007. [Online]. Available: https://web.archive.org/web/20071222072154/http://rpow.net/. [Accessed: 28-Sep-2018]

[34] S. Nakamoto, “Bitcoin v0.1 Released,” Jan. 2009 [Online]. Available: http://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html. [Accessed: 12-Feb-2016]

[35] R. L. Graham, N. Shahmehri, L. högskola, Sweden, and I. of Electrical and Electronics Engineers, Eds., *First International Conference on Peer-to-Peer Computing, 27-29 August 2001, Linköping, Sweden: Proceedings*. Los Alamitos, Calif: IEEE Computer Society, 2002.

[36] A. S. Tanenbaum and M. van Steen, *Distributed systems: Principles and paradigms*, 2nd ed. Upper Saddle RIiver, NJ: Pearson Prentice Hall, 2007.

[37] L. Lamport, “Time, Clocks, and the Ordering of Events in a Distributed System,” vol. 21, no. 7, p. 8, 1978.

[38] P. Kasireddy, “How Does Distributed Consensus Work?” *Medium*, 15-Dec-2018. [Online]. Available: https://medium.com/s/story/lets-take-a-crack-at-understanding-distributed-consensus-dad23d0dc95. [Accessed: 29-Oct-2019]

[39] C. Dwork, N. Lynch, and L. Stockmeyer, “Consensus in the presence of partial synchrony,” *J. ACM*, vol. 35, no. 2, pp. 288–323, Apr. 1988 [Online]. Available: http://portal.acm.org/citation.cfm?doid=42282.42283. [Accessed: 29-Oct-2019]

[40] J. Fischer and A. Lynch, “Impossibility of Distributed Consensuswith One Faulty Process,” p. 9, 1985.

[41] L. Lamport, “Paxos Made Simple,” 01-Nov-2001. [Online]. Available: https://www.microsoft.com/en-us/research/uploads/prod/2016/12/paxos-simple-Copy.pdf. [Accessed: 08-Oct-2018]

[42] V. Zamfir, “A Template for Correct-by-Construction Consensus Protocols.” Ethereum Foundation, 01-Nov-2017.

[43] L. Lamport, R. Shostak, and M. Pease, “The Byzantine Generals Problem,” *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, Jul. 1982 [Online]. Available: http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf. [Accessed: 18-Feb-2016]

[44] L. Lamport, “Proving the Correctness of Multiprocess Programs,” *IEEE Transactions on Software Engineering*, vols. SE-3, no. 2, pp. 125–143, Mar. 1977 [Online]. Available: http://ieeexplore.ieee.org/document/1702415/. [Accessed: 30-Oct-2019]

[45] M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance,” p. 14, Feb. 1999.

[46] Bitcoin Wiki, “Proof of Burn - Bitcoin Wiki,” Nov. 2015 [Online]. Available: https://en.bitcoin.it/wiki/Proof_of_burn. [Accessed: 26-Feb-2016]

[47] Bitcoin Wiki, “Controlled Supply - Bitcoin Wiki,” Apr. 2016 [Online]. Available: https://en.bitcoin.it/wiki/Controlled_supply. [Accessed: 27-Apr-2016]

[48] Bitcoin Wiki, “Transaction Fees - Bitcoin Wiki,” Mar. 2016 [Online]. Available: https://en.bitcoin.it/wiki/Transaction_fees. [Accessed: 27-Apr-2016]

[49] C. R. Harvey, “Bitcoin Myths and Facts,” 2014. [Online]. Available: http://bit.ly/2cHRu90. [Accessed: 24-Feb-2016]

[50] Gavin Andresen, “Seventy-Five, Twenty-Eight,” *Gavin Andresen on Svbtle*, May 2015 [Online]. Available: http://gavinandresen.ninja/seventyfive-twentyeight. [Accessed: 27-Apr-2016]

[51] Bitcoin, “Bitcoin Core,” 2016 [Online]. Available: https://bitcoin.org/en/bitcoin-core/. [Accessed: 29-Feb-2016]

[52] BitFury Group and Jeff Garzik, “Public versus Private Blockchains Part 1: Permissioned Blockchains White Paper,” Oct. 2015 [Online]. Available: http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf. [Accessed: 02-Mar-2016]

[53] Bitcoin, “Developer Guide - Bitcoin,” 2018. [Online]. Available: https://bitcoin.org/en/developer-guide#transactions. [Accessed: 01-Oct-2018]

[54] A. M. Antonopoulos, *Mastering Bitcoin*, First edition. Sebastopol CA: O’Reilly, 2015.

[55] Ethereum, “Ethereum White Paper,” Mar. 2016 [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper. [Accessed: 05-Apr-2016]

[56] R. C. Merkle, “PROTOCOLS FOR PUBUC KEY CRYPTOSYSTEMS,” 1980. [Online]. Available: http://www.merkle.com/papers/Protocols.pdf. [Accessed: 02-Mar-2016]

[57] Marcin Andrychowicz and Stefan Dziembowski, “Distributed Cryptography Based on the Proofs of Work.” University of Warsaw, 2014 [Online]. Available: http://eprint.iacr.org/2014/796.pdf. [Accessed: 25-Feb-2016]

[58] J. R. Douceur, “The Sybil Attack.” Microsoft Research, 2002 [Online]. Available: http://research.microsoft.com/pubs/74220/IPTPS2002.pdf. [Accessed: 25-Feb-2016]

[59] G. Greenspan, “Ending the Bitcoin vs Blockchain Debate | MultiChain,” Jul. 2015 [Online]. Available: http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/. [Accessed: 14-Feb-2016]

[60] A. Guadamuz and C. Marsden, “Blockchains and Bitcoin: Regulatory Responses to Cryptocurrencies,” *First Monday*, vol. 20, no. 12, Dec. 2015 [Online]. Available: http://journals.uic.edu/ojs/index.php/fm/article/view/6198. [Accessed: 24-Feb-2016]

[61] Ethereum, *Modified GHOST Implementation*. ethereum, 2018 [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper#modified-ghost-implementation. [Accessed: 02-Oct-2018]

[62] Y. Sompolinsky and A. Zohar, “Accelerating Bitcoin’s Transaction Processing. Fast Money Grows on Trees, Not Chains,” 881, 2013 [Online]. Available: http://eprint.iacr.org/2013/881. [Accessed: 02-Oct-2018]

[63] Ethereum, “Gas and Ether,” 2016. [Online]. Available: http://ethdocs.org/en/latest/ether.html#gas-and-ether. [Accessed: 11-Sep-2018]

[64] N. Szabo, “Smart Contracts,” 1994. [Online]. Available: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. [Accessed: 01-Oct-2018]

[65] E. Ostrom, “Beyond Markets and States: Polycentric Governance of Complex Economic Systems,” p. 37, Dec. 2009.

[66] H. Karlstrom, “Do Libertarians Dream of Electric Coins? The Material Embeddedness of Bitcoin,” *Distinktion: Scandinavian Journal of Social Theory*, vol. 15, no. 1, pp. 23–36, Jan. 2014 [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/1600910X.2013.870083. [Accessed: 26-Jun-2016]

[67] D. Boaz and D. Kirby, “The Libertarian Vote,” *Cato Institute*, Oct. 2006 [Online]. Available: http://www.cato.org/publications/policy-analysis/libertarian-vote. [Accessed: 30-Jun-2016]

[68] Libertarian Party, “Libertarian Party Platform,” *Libertarian Party*, May 2016 [Online]. Available: https://www.lp.org/platform. [Accessed: 11-Jul-2016]

[69] Bitcoin Wiki, “Controlled Supply - Bitcoin Wiki,” Jun. 2016 [Online]. Available: https://en.bitcoin.it/wiki/Controlled_supply. [Accessed: 23-Jul-2016]

[70] Bank of Canada, “Seigniorage,” 2013 [Online]. Available: http://www.bankofcanada.ca/wp-content/uploads/2010/11/seigniorage.pdf. [Accessed: 04-Aug-2016]

[71] Julian Martinez, “XRP: Math-Based Currency,” *Ripple*, Feb. 2015 [Online]. Available: https://ripple.com/knowledge_center/math-based-currency-2/. [Accessed: 23-Jul-2016]

[72] D. Yermack, “Is Bitcoin a Real Currency? An Economic Appraisal,” National Bureau of Economic Research, 2013 [Online]. Available: http://www.nber.org/papers/w19747. [Accessed: 21-Jul-2016]

[73] Oxford Dictionary, “Socialism,” 2016. [Online]. Available: http://www.oxforddictionaries.com/definition/english/socialism. [Accessed: 28-Jun-2016]

[74] F. Stadler, “Digital Commons: A dictionary entry,” 22-Apr-2010. [Online]. Available: http://felix.openflows.com/node/137. [Accessed: 10-Oct-2017]

[75] P. Freire, *Pedagogy of the Oppressed*, 30th anniversary edition. New York: Continuum, 2000.

[76] S. Metcalf, “Neoliberalism: The idea that swallowed the world,” *The Guardian: News*, 18-Aug-2017 [Online]. Available:

http://www.theguardian.com/news/2017/aug/18/neoliberalism-the-idea-that-changed-the-world. [Accessed: 09-Feb-2018]

[77] H. Gintis, *The bounds of reason: Game theory and the unification of the behavioral sciences*. Princeton, N.J: Princeton University Press, 2009.

[78] D. Bollier, *Think like a commoner: A short introduction to the life of the commons*. Gabriola, British Columbia: New Society Publishers, 2014.

[79] M. Castells, *The Rise of the Network Society The Information Age: Economy, Society, and Culture Volume I*. Somerset: Wiley, 2011.

[80] P2P Foundation, "Our Guiding Principles," *P2P Foundation*, 2017. [Online]. Available: https://p2pfoundation.net/infrastructure/our-guiding-principles. [Accessed: 05-Oct-2017]

[81] G. Hardin, "The Tragedy of the Commons," *Science*, vol. 162, no. 3859, pp. 1243–1248, Dec. 1968 [Online]. Available: http://www.sciencemag.org/cgi/doi/10.1126/science.162.3859.1243. [Accessed: 28-Sep-2018]

[82] C. J. Dahlman, "The tragedy of the commons that wasn't: On technical solutions to the institutions game," *Population and Environment*, vol. 12, no. 3, pp. 285–296, Mar. 1991 [Online]. Available: http://link.springer.com/10.1007/BF01357919. [Accessed: 28-Sep-2018]

[83] E. Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge: Cambridge University Press, 2015 [Online]. Available: http://ezproxy.eui.eu/login?url=http://dx.doi.org/10.1017/CBO9781316423936. [Accessed: 02-Oct-2017]

[84] KOORI HISTORY, "Were Aboriginal Australians Nomadic: Fact or Fiction?" *Koori History - Aboriginal History of South Eastern Australia*, 11-May-2016. [Online]. Available: http://koorihistory.com/aboriginal-nomadic/. [Accessed: 23-Nov-2017]

[85] P. Linebaugh and M. Rediker, *The Many-Headed Hydra: Sailors, Slaves, Commoners, and the Hidden History of the Revolutionary Atlantic*. Boston: Beacon Press, 2000.

[86] Marshall Sahlins, "The Original Affluent Society," 1974. [Online]. Available: http://www.primitivism.com/original-affluent.htm. [Accessed: 23-Nov-2017]

[87] J. Suzman, "Why 'Bushman banter' was crucial to hunter-gatherers' evolutionary success," *The Guardian: Inequality*, 29-Oct-2017 [Online]. Available: http://www.theguardian.com/inequality/2017/oct/29/why-bushman-banter-was-crucial-to-hunter-gatherers-evolutionary-success. [Accessed: 19-Nov-2017]

[88] D. J. Langton and D. G. Jones, "Forests and Chases: Henry III's Charter of the Forest," *St John's College, University of Oxford - Forests and Chases in England and Wales to c. 1850*, 2017. [Online]. Available: http://info.sjc.ox.ac.uk/forests/Carta.htm. [Accessed: 08-Oct-2017]

[89] J. C. Holt, *Magna Carta*, 2nd ed. Cambridge: Cambridge University Press, 1992 [Online]. Available: http://ebooks.cambridge.org/ref/id/CBO9781107049956. [Accessed: 06-Nov-2017]

[90] J. A. Yelling, *Common field and enclosure in England, 1450-1850*. London: Macmillan, 1977.

[91] S. E. Schoenherr, "The Digital Revolution," 05-May-4AD. [Online]. Available: https://web.archive.org/web/20081007132355/http://history.sandiego.edu/gen/recording/digital.html. [Accessed: 08-Oct-2017]

[92] M. Hilbert, "Toward a Conceptual Framework for ICT for Development: Lessons Learned from the Cube Framework Used in Latin America (English)," *Information Technologies & International Development*, vol. 8, no. 4, pp. pp. 243–259, Dec. 2012 [Online]. Available: http://itidjournal.org/index.php/itid/article/view/967. [Accessed: 08-Oct-2017]

[93] D. Bollier, *Viral spiral: How the commoners built a digital republic of their own*. New York: New Press, 2008.

[94] Internet World Stats, "World Internet Users Statistics and 2017 World Population Stats," 2017. [Online]. Available: http://www.internetworldstats.com/stats.htm. [Accessed: 08-Oct-2017]

[95] Apache, "The Apache HTTP Server Project," 2017. [Online]. Available: https://httpd.apache.org/. [Accessed: 15-Nov-2017]

[96] J. Nussbaum, "Apple Computer, Inc. v. Franklin Computer Corporation Puts the Byte Back into Copyright Protection for Computer Programs," *Golden Gate University Law Review*, vol. 14, no. 2, Jan. 1984 [Online]. Available: https://digitalcommons.law.ggu.edu/ggulrev/vol14/iss2/3

[97] E. Raymond, "The hacker Jargon File, version 4.3.3." 20-Sep-2002 [Online]. Available: http://www.proselex.net/documents/the%20new%20hacker's%20dictionary.pdf. [Accessed: 08-Nov-2017]

[98] Open Source Initiative, "Open Source Initiative," 2017. [Online]. Available: https://opensource.org/. [Accessed: 18-Oct-2017]

[99] D. Bollier, "The Rediscovery of the Commons," *UPGRADE*, vol. 4, no. 3, Jun. 2003 [Online]. Available: http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4979/up4-3Bollier.pdf?sequence=1&isAllowed=y. [Accessed: 10-Aug-2017]

[100] C. M. Kelty, *Two bits: The cultural significance of free software*. Durham: Duke University Press, 2008.

[101] Commons Transition, "Organizing and Governing the Commons: A Coop-Commons Multilevel Dialogue with Municipalities and Labour," *Commons Transition*, 16-Nov-2017. [Online]. Available: http://commonstransition.org/organizing-and-governing-the-commons-a-coop-commons-multilevel-dialogue-with-municipalities-and-labour/. [Accessed: 16-Nov-2017]

[102] F. Stalder, “Manuel Castells and the Theory of the Network Society, Polity Press, 2006,” 2006. [Online]. Available: http://felix.openflows.com/html/castells_polity.html. [Accessed: 11-Oct-2017]

[103] M. Gartler, “Rhizome | The Chicago School of Media Theory,” 2017. [Online]. Available: https://lucian.uchicago.edu/blogs/mediatheory/keywords/rhizome/. [Accessed: 16-Nov-2017]

[104] A. Grear, “Book review: David Bollier, Think Like a Commoner: A Short Introduction to the Life of the Commons (New Society Publishers, Gabriola Island, Canada 2014) 192 pp.” *Journal of Human Rights and the Environment*, vol. 5, no. 2, pp. 213–219, Sep. 2014 [Online]. Available: https://www.elgaronline.com/abstract/journals/jhre/5-2/jhre.2014.03.06.xml . [Accessed: 04-Oct-2017]

[105] GNU, “What is free software?” 04-Apr-2017. [Online]. Available: https://www.gnu.org/philosophy/free-sw.en.html. [Accessed: 19-Nov-2017]

[106] Y. Benkler, “Coase’s Penguin, or, Linux and The Nature of the Firm,” *Yale L.J.*, vol. 112, pp. 369–446, 2002–2003.

[107] D. Kreiss, M. Finn, and F. Turner, “The limits of peer production: Some reminders from Max Weber for the network society,” *New Media & Society*, vol. 13, no. 2, pp. 243–259, Mar. 2011 [Online]. Available: http://journals.sagepub.com/doi/10.1177/1461444810370951. [Accessed: 06-Jun-2019]

[108] H. Nicholas, *Marx’s theory of price and its modern rivals*. Houndmills, Basingstoke, Hampshire, England ; New York, NY: Palgrave Macmillan, 2011.

[109] Danyl Strype, “Free to Know or Free to Own? Convergence of Free and Slow Culture in Global Relocalisation,” 05-Sep-2010. [Online]. Available: https://www.coactivate.org/people/strypey/abstract. [Accessed: 15-Nov-2017]

[110] G. von Krogh and E. von Hippel, “The Promise of Research on Open Source Software,” *Management Science*, vol. 52, pp. 975–983, 2006.

[111] Brett Scott, “How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?” Feb. 2016 [Online]. Available: http://www.unrisd.org/brett-scott. [Accessed: 20-Jul-2016]

[112] Aaron Wright and Primavera de Filippi, “Decentralized Blockchain Technology and the Rise of Lex Cryptographia,” Mar. 2015 [Online]. Available: http://bit.ly/2cDOiqT. [Accessed: 03-Aug-2016]

[113] B. Scott, “How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?” United Nations Research Institute for Social Development, Feb-2016 [Online]. Available: http://www.unrisd.org/brett-scott. [Accessed: 20-Jul-2016]

[114] S. Huckle, “Bitcoin’s high energy consumption is a concern – but it may be a price worth paying,” *The Conversation*, 2018. [Online]. Available:

http://theconversation.com/bitcoins-high-energy-consumption-is-a-concern-but-it-may-be-a-price-worth-paying-106282. [Accessed: 05-Jun-2019]

[115] Intergovernmental Panel on Climate Change, *Climate Change 2014: Synthesis Report. Contribution of Working Groups I, II and III to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change*. Geneva, Switzerland: Intergovernmental Panel on Climate Change, 2014.

[116] S. Sherwood, "Science controversies past and present," *Physics Today*, vol. 64, no. 10, pp. 39–44, Oct. 2011 [Online]. Available: https://physicstoday.scitation.org/doi/10.1063/PT.3.1295. [Accessed: 30-May-2019]

[117] S. R. Weart, *The discovery of global warming*, Rev. and expanded ed. Cambridge, Mass: Harvard University Press, 2008.

[118] The White House, *Restoring the quality of our environment*. [Washington], 1965 [Online]. Available: http://hdl.handle.net/2027/uc1.b4116127

[119] M. Bookchin, "Ecology and Revolutionary Thought," 1964. [Online]. Available: http://dwardmac.pitzer.edu/Anarchist_Archives/bookchin/ecologyandrev.html. [Accessed: 30-May-2019]

[120] J. S. Sawyer, "Man-made Carbon Dioxide and the 'Greenhouse' Effect," *Nature*, vol. 239, no. 5366, pp. 23–26, Sep. 1972 [Online]. Available: http://www.nature.com/articles/239023a0. [Accessed: 30-May-2019]

[121] D. H. Meadows and C. of Rome, Eds., *The Limits to growth: A report for the Club of Rome's project on the predicament of mankind*. New York: Universe Books, 1972.

[122] World Meteorological Organisation, "Declaration of the World Climate Conference," 1979. [Online]. Available: https://dgvn.de/fileadmin/user_upload/DOKUMENTE/WCC-3/Declaration_WCC1.pdf. [Accessed: 30-May-2019]

[123] N. H. Stern and Great Britain, Eds., *The Economics of Climate Change: The Stern Review*. Cambridge, UK ; New York: Cambridge University Press, 2007.

[124] United Nations Framework Convention on Climate Change, "The Paris Agreement," 22-Oct-2018. [Online]. Available: https://unfccc.int/process-and-meetings/the-paris-agreement/the-paris-agreement. [Accessed: 30-May-2019]

[125] BBC, *BBC Radio 4*. BBC, 2017 [Online]. Available: http://www.bbc.co.uk/programmes/b09gzj9j. [Accessed: 04-Dec-2017]

[126] World Meteorological Organization, "WMO Statement on the state of the global climate in 2018," p. 44, 2019.

[127] Letters, "Climate crisis and a betrayed generation," *The Guardian: Environment*, 01-Mar-2019 [Online]. Available:

https://www.theguardian.com/environment/2019/mar/01/youth-climate-change-strikers-open-letter-to-world-leaders. [Accessed: 30-May-2019]

[128] I. Cohen and J. Heberle, “Youth Demand Climate Action in Global School Strike | Harvard Political Review,” 19-Mar-2019. [Online]. Available: http://harvardpolitics.com/united-states/youth-demand-climate-action-in-global-school-strike/. [Accessed: 30-May-2019]

[129] M. Bookchin, D. Bookchin, and B. Taylor, *The next revolution: Popular assemblies and the promise of direct democracy*. London ; New York: Verso, 2015.

[130] S. Sorrell, “Reducing energy demand: A review of issues, challenges and approaches,” *Renewable and Sustainable Energy Reviews*, vol. 47, pp. 74–82, Jul. 2015 [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1364032115001471. [Accessed: 20-Sep-2019]

[131] Benjamin D. Mazzotta, Bhaskar Chakravorti, R. Bijapurkar, Dr. Rajesh Shukla, Dr. K. Ramesha, Dr. Dhananjay Bapat, Dr. Deepankar Roy, Nikhil Joseph, Shalini Sharan, Ruben Korenke, and Siddharth Durgavanshi, “THE COST OF CASH IN INDIA,” *THE INSTITUTE FOR BUSINESS IN THE GLOBAL CONTEXT*, 2014. [Online]. Available: http://fletcher.tufts.edu/~/media/Fletcher/Microsites/Cost%20of%20Cash/COC-India-lowres.pdf. [Accessed: 19-Jan-2017]

[132] Global Innovation Exchange, “Beyond Cash,” 11-Jan-2016. [Online]. Available: https://www.globalinnovationexchange.org/beyond-cash. [Accessed: 19-Jan-2017]

[133] A. Demirguc-Kunt, L. Klapper, D. Singer, and P. V. Oudheusden, “The Global Findex Database 2014 - Measuring Financial Inclusion around the World,” Apr. 2015 [Online]. Available: http://documents.worldbank.org/curated/en/187761468179367706/pdf/WPS7255.pdf. [Accessed: 19-Jan-2017]

[134] J. Manyika, S. Lund, M. Singer, O. White, and C. Berry, “How Digital Finance Could Boost Growth in Emerging Economies | McKinsey & Company,” Sep. 2016 [Online]. Available: http://www.mckinsey.com/global-themes/employment-and-growth/how-digital-finance-could-boost-growth-in-emerging-economies. [Accessed: 19-Jan-2017]

[135] Times of India, “Learning with the Times: What Is Aadhaar?” *The Times of India*, Oct. 2010 [Online]. Available: http://timesofindia.indiatimes.com/india/Learning-with-the-Times-What-is-Aadhaar/articleshow/6680601.cms. [Accessed: 21-Jan-2017]

[136] Gopika Gopakumar, “Visa & MasterCard gone. Rupay card, bring it on,” *Moneycontrol.com*, 22-Jun-2011. [Online]. Available: http://www.moneycontrol.com/news/cnbc-tv18-comments/visamastercard-gone-rupay-card-bring-it-on_559115.html. [Accessed: 21-Jan-2017]

[137] George Mathew, “Check your cash, pre-2005 notes will not work after July,” *The Indian Express*, January 23, 2014 1:25 am. [Online]. Available: http://indianexpress.com/article/india/india-others/rbi-to-

withdraw-all-currency-notes-issued-before-2005-after-march/. [Accessed: 20-Jan-2017]

[138] Government of India, “Pradhan Mantri Jan Dhan Yojana,” 27AD–Aug-2014. [Online]. Available: http://pib.nic.in/newsite/erelease.aspx?relid=109113. [Accessed: 19-Jan-2017]

[139] Sai Nidhi, “Here’s what you need to know about the Digital India initiative | Latest News & Updates at Daily News & Analysis,” *dna*, 28-Sep-2015. [Online]. Available: http://www.dnaindia.com/money/report-here-s-what-you-need-to-know-about-the-digital-india-initiative-2129525. [Accessed: 21-Jan-2017]

[140] National Payments Corporation of India, “Unified Payments Interface (UPI),” 2016. [Online]. Available: http://www.npci.org.in/UPI_Background.aspx. [Accessed: 21-Jan-2017]

[141] PTI, “Government wants Aadhaar-enabled payment to replace debit, credit cards,” *The Indian Express*, December 2, 2016 9:24 am. [Online]. Available: http://indianexpress.com/article/business/banking-and-finance/government-wants-aadhaar-enabled-payment-to-replace-cards-4406261/. [Accessed: 21-Jan-2017]

[142] dipti jain, “Did Jan Dhan accounts really help in money laundering post demonetisation?” *http://www.livemint.com/*, 12-Jan-2017. [Online]. Available: http://www.livemint.com/Industry/PQwAM6rykFx2EDJsYzowVO/Did-Jan-Dhan-account-holders-help-in-money-laundering-postn.html. [Accessed: 20-Jan-2017]

[143] The Times of India, “400-1000% increase in digital transactions after demonetisation, says government - Times of India,” *The Times of India*, 09-Dec-2016. [Online]. Available: http://timesofindia.indiatimes.com/business/india-business/400-1000-increase-in-digital-transactions-after-demonetisation-says-government/articleshow/55897291.cms. [Accessed: 20-Jan-2017]

[144] W. Shepard, “One Month In, What’s The Impact Of India’s Demonetization Fiasco?” *Forbes*, 12-Dec-2016. [Online]. Available: http://www.forbes.com/sites/wadeshepard/2016/12/12/one-month-in-whats-the-impact-of-indias-demonetization-fiasco/. [Accessed: 20-Jan-2017]

[145] Special Correspondent, “With 220mn users, India is now world’s second-biggest smartphone market,” *The Hindu*, 03-Feb-2016 [Online]. Available: http://www.thehindu.com/news/cities/mumbai/business/with-220mn-users-india-is-now-worlds-secondbiggest-smartphone-market/article8186543.ece. [Accessed: 21-Jan-2017]

[146] Statista, “Internet usage in India,” *www.statista.com*, 2019. [Online]. Available: https://www.statista.com/topics/2157/internet-usage-in-india/. [Accessed: 21-May-2019]

[147] D. B. Nagle and S. M. Burstein, Eds., *The Ancient World: Readings in Social and Cultural History*, 4th ed. New York: Prentice Hall, 2010.

[148] E. L. Bernays and M. C. Miller, *Propaganda*. Brooklyn, N.Y: Ig Publishing, 2005.

[149] D. D. Clarke, “The corpse factory and the birth of fake news,” Feb. 2017 [Online]. Available: http://www.bbc.co.uk/news/entertainment-arts-38995205. [Accessed: 25-Feb-2017]

[150] A-Z Quotes, “Joseph Goebbels Quote,” *A-Z Quotes*, 2017. [Online]. Available: http://www.azquotes.com/quote/1419276. [Accessed: 04-Mar-2017]

[151] S. Davies, *Popular opinion in Stalin’s Russia: Terror, propaganda, and dissent, 1934-1941*. Cambridge ; New York: Cambridge University Press, 1997.

[152] I. Zasurskiĭ, *Media and Power in Post-Soviet Russia*. Armonk, N.Y: M.E. Sharpe, 2004.

[153] Office of the Historian, “Foreign Relations of the United States, 1945–1950, Emergence of the Intelligence Establishment.” 18-Jun-1948 [Online]. Available: https://history.state.gov/historicaldocuments/frus1945-50Intel/d292. [Accessed: 04-May-2017]

[154] R. W. McChesney, E. M. Wood, and J. B. Foster, Eds., *Capitalism and the information age: The political economy of the global communication revolution*. New York, NY: Monthly Review Press, 1998.

[155] Jane’s 360, “Acknowledgement of Russia’s Information Warfare Capability Indicates Its Strategic Importance and Impracticability of Maintaining Plausible,” Feb. 2017 [Online]. Available: http://www.janes.com/article/68267/acknowledgement-of-russia-s-information-warfare-capability-indicates-its-strategic-importance-and-impracticability-of-maintaining-plausible-deniability-policy. [Accessed: 04-May-2017]

[156] I. Khaldarova and M. Pantti, “Fake News: The narrative battle over the Ukrainian conflict,” *Journalism Practice*, vol. 10, no. 7, pp. 891–901, Oct. 2016 [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/17512786.2016.1163237. [Accessed: 02-Mar-2017]

[157] D. Zhao, *The power of Tiananmen: State-society relations and the 1989 Beijing student movement*. Chicago: University of Chicago Press, 2001.

[158] L. Lim, “Opinion | After Tiananmen, China Conquers History Itself,” *The New York Times: Opinion*, 03-Jun-2019 [Online]. Available: https://www.nytimes.com/2019/06/02/opinion/tiananmen-square-china.html. [Accessed: 03-Jun-2019]

[159] R. Love, “Before Jon Stewart,” *Columbia Journalism Review*, Apr-2007. [Online]. Available: http://www.cjr.org/feature/before_jon_stewart.php. [Accessed: 01-Mar-2017]

[160] *Fake news series part two*. 19:00 00:41:21-00:55:54: Channel 4, 2017 [Online]. Available: https://learningonscreen.ac.uk/ondemand/index.php/clip/90422

[161] G. Orwell, *1984: A Novel; Revised and Updated Bibliography*. New York [u.a.: New American Library, 1985.

[162] L. I. I. Staff, “First Amendment.” 05-Feb-2010 [Online]. Available: https://www.law.cornell.edu/constitution/first_amendment. [Accessed: 01-Mar-2017]

[163] E. Charlton, “Fake news: What it is, and how to spot it,” *World Economic Forum*, 06-Mar-2019. [Online]. Available: https://www.weforum.org/agenda/2019/03/fake-news-what-it-is-and-how-to-spot-it/. [Accessed: 22-May-2019]

[164] J. Goodfellow, “Only 4% of people can distinguish fake news from truth, Channel 4 study finds,” *The Drum*, 06-Feb-2017 [Online]. Available: http://www.thedrum.com/news/2017/02/06/only-4-people-can-distinguish-fake-news-truth-channel-4-study-finds. [Accessed: 23-Mar-2017]

[165] D. A. Scheufele and N. M. Krause, “Science audiences, misinformation, and fake news,” *PNAS*, vol. 116, no. 16, pp. 7662–7669, Apr. 2019 [Online]. Available: https://www.pnas.org/content/116/16/7662. [Accessed: 22-May-2019]

[166] R. Botsman, *Who can you trust?: How technology brought us together – and why it could drive us apart*. 2018.

[167] R. DiResta, “The Information War Is On. Are We Ready For It?” *Wired*, 03-Aug-2018 [Online]. Available: https://www.wired.com/story/misinformation-disinformation-propaganda-war/. [Accessed: 22-May-2019]

[168] C. Silverman, “This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook,” *BuzzFeed*, 16-Nov-2016. [Online]. Available: https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook. [Accessed: 09-May-2017]

[169] J. Weedon, W. Nuland, and A. Stamos, “Facebook and Information Operations,” 2017 [Online]. Available: https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf. [Accessed: 08-May-2017]

[170] D. MacIntyre, “Facebook - the secret election weapon,” *BBC News: UK*, 08-May-2017 [Online]. Available: http://www.bbc.co.uk/news/uk-39830727. [Accessed: 08-May-2017]

[171] Mark Zuckerberg, “What we’re doing about misinformation,” 19-Nov-2016. [Online]. Available: https://www.facebook.com/zuck/posts/10103269806149061?pnref=story. [Accessed: 09-May-2017]

[172] Drew Harwell, “AI will solve Facebook’s most vexing problems, Mark Zuckerberg says. Just don’t ask when or how. - The Washington Post,” 11-

Apr-2018. [Online]. Available: https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/ai-will-solve-facebooks-most-vexing-problems-mark-zuckerberg-says-just-dont-ask-when-or-how/?noredirect=on&utm_term=.8f4f02e2aa18. [Accessed: 23-May-2019]

[173] V. L. Rubin, Y. Chen, and N. J. Conroy, “Deception Detection for News: Three Types of Fakes: Deception Detection for News: Three Types of Fakes,” *Proceedings of the Association for Information Science and Technology*, vol. 52, no. 1, pp. 1–4, 2015 [Online]. Available: http://doi.wiley.com/10.1002/pra2.2015.145052010083. [Accessed: 19-Sep-2017]

[174] S. Missaoui, M. Gutierrez-Lopez, A. MacFarlane, S. Makri, C. Porlezza, and G. Cooper, “How to Blend Journalistic Expertise with Artificial Intelligence for Research and Verifying News Stories?” p. 5, 2019.

[175] K. Shu, A. Sliva, S. Wang, J. Tang, and H. Liu, “Fake News Detection on Social Media: A Data Mining Perspective,” p. 15, 2017.

[176] D. Boyd and K. Crawford, “Six Provocations for Big Data,” *SSRN Electronic Journal*, 2011 [Online]. Available: http://www.ssrn.com/abstract=1926431. [Accessed: 20-Sep-2017]

[177] R. Waugh, “Can AI really detect fake news on social media?” 06-Mar-2019. [Online]. Available: https://www.telegraph.co.uk/technology/information-age/can-artificial-intelligence-detect-fake-news/. [Accessed: 23-May-2019]

[178] GOV.UK, “Official Development Assistance - GOV.UK,” 2018. [Online]. Available: https://www.gov.uk/government/publications/official-development-assistance/official-development-assistance. [Accessed: 24-Mar-2018]

[179] C. Morris, “Reality Check: How much does the UK spend on overseas aid?” *BBC News: UK Politics*, 20-Apr-2017 [Online]. Available: http://www.bbc.co.uk/news/uk-politics-39658907. [Accessed: 24-Mar-2018]

[180] B. D. B. for MailOnline, “Strip aid money from corrupt countries urges David Cameron,” *Mail Online*, 14-Mar-2018. [Online]. Available: http://www.dailymail.co.uk/news/article-5498055/Strip-aid-money-corrupt-countries-urges-David-Cameron.html. [Accessed: 24-Mar-2018]

[181] World Humanitarian Summit, “Commitments to Action - World Health Summit, Istanbul, 23-24 May 2016,” *Agenda for Humanity*, 08-Sep-2016. [Online]. Available: https://www.agendaforhumanity.org/sites/default/files/resources/2017/Jul/WHS_commitment_to_Action_8September2016.pdf. [Accessed: 24-May-2019]

[182] Development Initiatives, “Baseline report - Implementing and monitoring the Grand Bargain commitment on transparency,” Jun-2017. [Online]. Available: http://devinit.org/wp-content/uploads/2017/06/Baseline-report_-implementing-and-monitoring-the-Grand-Bargain-commitment-on-transparency.pdf. [Accessed: 25-May-2019]

[183] Development Initiatives, UN Office for the Coordination of Humanitarian Affairs, Inter-Agency Standing Committee, and Humanitarian Financing Task Team, “Improving humanitarian transparency with the International Aid Transparency Initiative (IATI) and the UN OCHA Financial Tracking Service (FTS),” Jul-2017. [Online]. Available: https://fts.unocha.org/sites/default/files/improving-humanitarian-transparency-with-the-iati-and-the-un-ocha-fts.pdf. [Accessed: 07-May-2019]

[184] UN Office for the Coordination of Humanitarian, “Improving Humanitarian Transparency with the International Aid Transparency Initiative (IATI) and the UN OCHA Financial Tracking Service (FTS),” Jul. 2017 [Online]. Available: https://fts.unocha.org/sites/default/files/improving-humanitarian-transparency-with-the-iati-and-the-un-ocha-fts.pdf. [Accessed: 24-Mar-2018]

[185] C. L. Owen, “UNDERSTANDING DESIGN RESEARCH : Toward an Achievement of Balance.” Japanese Society for the Science of Design, 1997 [Online]. Available: https://doi.org/10.11247/jssds.5.2_36. [Accessed: 07-Apr-2019]

[186] S. Gregor and A. R. Hevner, “Positioning and Presenting Design Science Research for Maximum Impact,” *MIS Quarterly*, vol. 37, pp. 337–355, 2013.

[187] S. Gregor and D. Jones, “The Anatomy of a Design Theory,” *Journal of the Association for Information Systems*, vol. 8, no. 5, May 2007 [Online]. Available: https://aisel.aisnet.org/jais/vol8/iss5/19

[188] M. Poppendieck, “Lean Software Development,” in *29th International Conference on Software Engineering (ICSE’07 Companion)*, 2007, pp. 165–166.

[189] M. Poppendieck and M. A. Cusumano, “Lean Software Development: A Tutorial,” *IEEE Softw.*, vol. 29, no. 5, pp. 26–32, Sep. 2012 [Online]. Available: http://ieeexplore.ieee.org/document/6226341/. [Accessed: 01-May-2019]

[190] The Lean Startup, “Methodology,” 2019. [Online]. Available: http://theleanstartup.com/principles. [Accessed: 02-May-2019]

[191] J. Mingers, “The Contribution of Critical Realism as an Underpinning Philosophy for OR/MS and Systems,” *The Journal of the Operational Research Society*, vol. 51, no. 11, p. 1256, Nov. 2000 [Online]. Available: https://www.jstor.org/stable/254211?origin=crossref. [Accessed: 09-Apr-2019]

[192] R. Levitas, *Utopia as Method*. London: Palgrave Macmillan UK, 2013 [Online]. Available: http://link.springer.com/10.1057/9781137314253. [Accessed: 20-Oct-2018]

[193] E. McKenna, *The task of Utopia: A pragmatist and feminist perspective*. 2001 [Online]. Available:

http://public.eblib.com/choice/publicfullrecord.aspx?p=1387276. [Accessed: 21-Oct-2018]

[194] M. Saunders, P. Lewis, and A. Thornhill, “Understanding Research Philosophies and Approaches,” *Research Methods for Business Students*, vol. 4, pp. 106–135, Jan. 2009.

[195] T. Burke, “About me too,” *Me Too Movement*, 2018. [Online]. Available: https://metoomvmt.org/about/. [Accessed: 22-Oct-2018]

[196] J. H. Maruska, “Feminist Ontologies, Epistemologies, Methodologies, and Methods in International Relations,” *Oxford Research Encyclopedia of International Studies*, Mar. 2010 [Online]. Available: http://internationalstudies.oxfordre.com/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-178. [Accessed: 22-Oct-2018]

[197] A. Miller, “To truly ‘man up,’ we, too, must fight sexism with more than outrage,” *thenewstribune*, 22-Oct-2017. [Online]. Available: https://www.thenewstribune.com/opinion/article180060591.html. [Accessed: 22-Oct-2018]

[198] G. Burrell and G. Morgan, *Sociological paradigms and organisational analysis: Elements of the sociology of corporate life*. London: Heinemann, 1979.

[199] A. Hern, “Bitcoin’s energy usage is huge – we can’t afford to ignore it,” *The Guardian: Technology*, 17-Jan-2018 [Online]. Available: https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency. [Accessed: 14-Oct-2019]

[200] S. Lee, “Bitcoin’s Energy Consumption Can Power An Entire Country – But EOS Is Trying To Fix That,” 19-Apr-2018. [Online]. Available: https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/#40b417921bc8. [Accessed: 14-Oct-2019]

[201] G.F, “Why bitcoin uses so much energy,” *The Economist*, 09-Jul-2018 [Online]. Available: https://www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy. [Accessed: 14-Oct-2019]

[202] M. J. Krause and T. Tolaymat, “Quantification of energy and carbon costs for mining cryptocurrencies,” *Nat Sustain*, vol. 1, no. 11, pp. 711–718, Nov. 2018 [Online]. Available: https://www.nature.com/articles/s41893-018-0152-7. [Accessed: 14-Oct-2019]

[203] OpenZeppelin, “Tokens - OpenZeppelin Docs,” 2019. [Online]. Available: https://docs.openzeppelin.com/contracts/2.x/tokens. [Accessed: 29-Aug-2019]

[204] International Energy Agency, “World Energy Balances - Overview.” 2019 [Online]. Available: https://webstore.iea.org/download/direct/2710?fileName=World_Energy_Balances_2019_Overview.pdf

[205] M. L. Katz and C. Shapiro, “Systems Competition and Network Effects,” *Journal of Economic Perspectives*, vol. 8, no. 2, pp. 93–115, Jun. 1994 [Online]. Available: https://www.aeaweb.org/articles?id=10.1257/jep.8.2.93. [Accessed: 14-Oct-2019]

[206] BBC News, “UK Parliament declares climate emergency,” *BBC News: UK Politics*, 01-May-2019 [Online]. Available: https://www.bbc.com/news/uk-politics-48126677. [Accessed: 14-Oct-2019]

[207] Sarah Bauder, “Largest Bitcoin Ownership Survey Reveals 6.2% Of Americans Own Bitcoin, While 7.3% Are Planning To Buy Some,” *Crypto Radar*, 30-Sep-2019. [Online]. Available: https://cryptoradar.org/largest-bitcoin-ownership-survey-reveals-6-2-of-americans-own-bitcoin-while-7-3-are-planning-to-buy-some/. [Accessed: 14-Oct-2019]

[208] Cane Island Alternative Advisors, “Why Bitcoin is Never Looking Back,” *Medium*, 09-Oct-2019. [Online]. Available: https://medium.com/@cane.island/why-bitcoin-is-never-looking-back-f06ab333742e. [Accessed: 14-Oct-2019]

[209] Policonomics, “Surplus | Policonomics,” 2017. [Online]. Available: https://policonomics.com/surplus/. [Accessed: 14-Oct-2019]

[210] A. Zmudzinski, “Miami International Airport Gets Its First Bitcoin ATM,” *Cointelegraph*, 16-Oct-2019. [Online]. Available: https://cointelegraph.com/news/miami-international-airport-gets-its-first-bitcoin-atm. [Accessed: 16-Oct-2019]

[211] B. Gehring, “How Ripple Works.” 16-Oct-2014 [Online]. Available: https://ripple.com/knowledge_center/how-ripple-works/. [Accessed: 23-Jul-2016]

[212] F. Martin, *Money: The Unauthorised Biography*. 2014.

[213] Z. Pozsar and M. Singh, “The Nonbank-Bank Nexus and the Shadow Banking System,” *IMF Working Papers*, pp. 1–18, 2011 [Online]. Available: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1971440. [Accessed: 21-Jul-2016]

[214] J. Rifkin, *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism*. New York, NY: Palgrave Macmillan, 2014.

[215] P. Alessandri and A. G. Haldane, *Banking on the State*. Bank of England London, 2009 [Online]. Available: http://qed.econ.queensu.ca/faculty/milne/870/Bank%20on%20the%20State.pdf. [Accessed: 21-Jul-2016]

[216] A. Savelyev, “Copyright in the blockchain era: Promises and challenges,” p. 12, 2018.

[217] Libra Association, “Libra White Paper,” *Libra.org*, 2019. [Online]. Available: https://libra.org/en-US/white-paper/. [Accessed: 23-Jun-2019]

[218] M. Mellor, “Neoliberalism has tricked us into believing a fairytale about where money comes from,” *The Conversation*, 22-Jun-2019. [Online]. Available: http://theconversation.com/neoliberalism-has-tricked-us-into-believing-a-fairytale-about-where-money-comes-from-113783. [Accessed: 24-Jun-2019]

[219] M. McLeay and A. Radia, “Money creation in the modern economy.” 2014.

[220] D. Clarke, “Why we must stop Facebook’s attempt to hijack our money, before it’s too late,” *openDemocracy*, 21-Jun-2019. [Online]. Available: https://www.opendemocracy.net/en/oureconomy/why-we-must-stop-facebooks-attempt-hijack-our-money-its-too-late/. [Accessed: 25-Jun-2019]

[221] F. Arisandi, “5 countries that are going big on cryptocurrency adoption,” 18-Mar-2019. [Online]. Available: https://www.chepicap.com/en/news/8157/crypto-mass-adoption-may-be-far-but-these-countries-are-paving-the-way.html. [Accessed: 16-May-2019]

[222] R. Krygier, “Venezuela launches the ‘petro,’ its cryptocurrency,” *Washington Post*, 20-Feb-2018. [Online]. Available: https://www.washingtonpost.com/news/worldviews/wp/2018/02/20/venezuela-launches-the-petro-its-cryptocurrency/. [Accessed: 16-May-2019]

[223] S. Shane, “From Headline to Photograph, a Fake News Masterpiece,” *The New York Times*, 18-Jan-2017 [Online]. Available: https://www.nytimes.com/2017/01/18/us/fake-news-hillary-clinton-cameron-harris.html. [Accessed: 05-Feb-2017]

[224] J. Walker, “Birmingham Mail Photo Used in a ’fake News’ Trump Story Shared with 6 Million,” *birminghammail*, 19-Jan-2017 [Online]. Available: http://www.birminghammail.co.uk/news/midlands-news/birmingham-mail-photo-used-fake-12476900. [Accessed: 27-Sep-2017]

[225] PREMIS Editorial Committee, “The PREMIS Data Dictionary Version 3.0,” Nov-2015. [Online]. Available: https://www.loc.gov/standards/premis/v3/premis-3-0-final.pdf. [Accessed: 29-Jun-2017]

[226] W3C, “Data on the Web - Best Practices,” 24-Feb-2015. [Online]. Available: https://www.w3.org/TR/2015/WD-dwbp-20150224/. [Accessed: 11-May-2017]

[227] E. Mannens, S. Coppens, R. Verborgh, L. Hauttekeete, D. Van Deursen, and R. Van de Walle, “Automated Trust Estimation in Developing Open News Stories: Combining Memento and Provenance,” 2012, pp. 122–127 [Online]. Available: http://ieeexplore.ieee.org/document/6341562/. [Accessed: 22-Sep-2017]

[228] Ujo Music, “Rebuilding the music industry on the blockchain,” *Ujo Music*, 2015. [Online]. Available: //ujomusic.com/. [Accessed: 29-May-2016]

[229] J. Bertolami, “Perceptual Hashing,” 28-May-2014. [Online]. Available: http://bertolami.com/index.php?engine=blog&content=posts&detail=perceptual-hashing. [Accessed: 24-Sep-2017]

[230] W. Shang, M. Liu, W. Lin, and M. Jia, “Tracing the Source of News Based on Blockchain,” in *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, 2018, pp. 377–381.

[231] S. Corbet, B. Lucey, A. Urquhart, and L. Yarovaya, “Cryptocurrencies as a financial asset: A systematic analysis,” *International Review of Financial Analysis*, vol. 62, pp. 182–199, Mar. 2019 [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1057521918305271. [Accessed: 15-Oct-2019]

[232] G. Coppi and L. Fast, “Blockchain and distributed ledger technologies in the humanitarian sector,” p. 46, Feb. 2019.

[233] Transparency International, “What is Corruption?” 2018. [Online]. Available: https://www.transparency.org/what-is-corruption#what-is-transparency. [Accessed: 24-Mar-2018]

[234] V. Kostakis, A. Roos, and M. Bauwens, “Towards a political ecology of the digital economy: Socio-environmental implications of two competing value models,” *Environmental Innovation and Societal Transitions*, vol. 18, pp. 82–100, Mar. 2016 [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S2210422415300150. [Accessed: 21-Dec-2017]

[235] M. Weber, *The Protestant ethic and the spirit of Capitalism*. CreateSpace Independent Publishing Platform, 2013.

[236] Max Weber, *Max Weber Economy and Society*. 1978 [Online]. Available: http://archive.org/details/MaxWeberEconomyAndSociety. [Accessed: 06-Jun-2019]

[237] M. H. Jarrahi, G. Philips, W. Sutherland, S. Sawyer, and I. Erickson, “Personalization of knowledge, personal knowledge ecology, and digital nomadism,” *Journal of the Association for Information Science and Technology*, vol. 70, no. 4, pp. 313–324, 2019 [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/asi.24134. [Accessed: 07-Jun-2019]

[238] J. Howison and K. Crowston, “Collaboration Through Open Superposition: A Theory of the Open Source Way,” *MIS Quarterly*, vol. 38, no. 1, pp. 29–50, Jan. 2014 [Online]. Available: https://misq.org/collaboration-through-open-superposition.html. [Accessed: 08-Jun-2019]

[239] M. Hoyles, “How the tech giants co-opted the world of open source,” *NS Tech*, 09-Nov-2018. [Online]. Available: https://tech.newstatesman.com/guest-opinion/red-hat-ibm-acquisition-open-source. [Accessed: 07-Jun-2019]

[240] D. H. Meadows and D. Wright, *Thinking in systems: A primer*. London [u.a.]: Earthscan, 2009.

[241] R. Dunbar, “Neocortex size as a constraint on group size in primates,” *Journal of Human Evolution*, vol. 22, no. 6, pp. 469–493, Jun. 1992 [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/004724849290081J. [Accessed: 09-Jun-2019]

[242] A. Hernando, D. Villuendas, C. Vesperinas, M. Abad, and A. Plastino, “Unravelling the size distribution of social groups with information theory on complex networks,” May 2009 [Online]. Available: http://arxiv.org/abs/0905.3704. [Accessed: 09-Jun-2019]

[243] H. Chesbrough, “Open Innovation: A New Paradigm for Understanding Industrial Innovation,” p. 27, Oct. 2005.

[244] E. von Hippel, “Open Source Software and the ‘Private-Collective’ Innovation Model: Issues for Organization Science,” 30-Apr-2002. [Online]. Available: https://evhippel.files.wordpress.com/2013/08/private-collective-model-os.pdf. [Accessed: 08-Jun-2019]

[245] Karl Marx, *Capital: A Critique of Political Economy. Volume One*. Progress Publishers, 1887 [Online]. Available: https://www.marxists.org/archive/marx/works/1867-c1/index.htm. [Accessed: 13-Jul-2016]

[246] N. S. Arnold, “Marx, Central Planning, and Utopian Socialism,” *Social Philosophy and Policy*, vol. 6, no. 02, p. 160, Mar. 1989 [Online]. Available: http://www.journals.cambridge.org/abstract_S0265052500000686. [Accessed: 13-Jul-2016]

[247] H.-j. Chang, *Economics: The user’s guide: A Pelican introduction*. London: Pelican Books, 2014.

[248] V. Narwal, M. H. Salih, J. A. Lopez, A. Ortega, J. O’Donovan, T. Höllerer, and S. Savage, “Automated Assistants to Identify and Prompt Action on Visual News Bias,” 2017, pp. 2796–2801 [Online]. Available: http://dl.acm.org/citation.cfm?doid=3027063.3053227. [Accessed: 22-Sep-2017]

[249] C. Sun and R. Nevatia, “Large-scale web video event classification by use of Fisher Vectors,” 2013, pp. 15–22 [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6474994. [Accessed: 24-Sep-2017]

[250] L. Liu, P. Wang, C. Shen, L. Wang, A. van den Hengel, C. Wang, and H. T. Shen, “Compositional Model Based Fisher Vector Coding for Image Classification,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 1–1, 2017 [Online]. Available: http://ieeexplore.ieee.org/document/7812753/. [Accessed: 24-Sep-2017]

[251] rfraimow, “Adventures in Perceptual Hashing,” *AAPB National Digital Stewardship Residency*, 20-Apr-2017. [Online]. Available: https://ndsr.americanarchive.org/2017/04/20/adventures-in-perceptual-hashing/. [Accessed: 24-Sep-2017]

[252] R. W. Hamming, “Error Detecting and Error Correcting Codes,” *Bell System Technical Journal*, vol. 29, no. 2, pp. 147–160, Apr. 1950 [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6772729. [Accessed: 27-Sep-2017]

[253] M. Duffield, “Governing the Borderlands: Decoding the Power of Aid,” *Disasters*, vol. 25, no. 4, pp. 308–320, 2001 [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/1467-7717.00180. [Accessed: 03-Nov-2019]

[254] K. Lewin, “Action Research and Minority Problems,” *Journal of Social Issues*, vol. 2, no. 4, pp. 34–46, Nov. 1946 [Online]. Available: http://doi.wiley.com/10.1111/j.1540-4560.1946.tb02295.x. [Accessed: 10-Feb-2020]

[255] M. Lawson, M.-K. Chan, F. Rhodes, A. Parvez Butt, A. Marriott, E. Ehmke, D. Jacobs, J. Seghers, J. Atienza, and R. Gowland, “Public Good or Private Wealth?” Oxfam, Jan. 2019 [Online]. Available: http://hdl.handle.net/10546/620599. [Accessed: 30-May-2019]

[256] World Bank, *Piecing Together the Poverty Puzzle*. The World Bank, 2018 [Online]. Available: http://elibrary.worldbank.org/doi/book/10.1596/978-1-4648-1330-6. [Accessed: 30-May-2019]

[257] P. Alston, “Statement on Visit to the United Kingdom, by Professor Philip Alston, United Nations Special Rapporteur on extreme poverty and human rights,” 16-Nov-2018. [Online]. Available: https://www.ohchr.org/Documents/Issues/Poverty/EOM_GB_16Nov2018.pdf. [Accessed: 30-May-2019]

[258] A. Pazaitis, P. De Filippi, and V. Kostakis, “Blockchain and Value Systems in the Sharing Economy: The Illustrative Case of Backfeed,” *Technological Forecasting and Social Change*, vol. 125, pp. 105–115, Dec. 2017 [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0040162517307084. [Accessed: 21-Dec-2017]

[259] I. Bogost, “The Nomad Who’s Exploding the Internet Into Pieces,” *The Atlantic*, 22-May-2017. [Online]. Available: https://www.theatlantic.com/technology/archive/2017/05/meet-the-counterantidisintermediationists/527553/. [Accessed: 14-Jun-2019]

[260] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. Boca Raton: CRC Press, 1997.

[261] Dr Konstantin Blyuss, “Cryptography - Lecture Notes.” 2016.

[262] Gavin Wood, “Ethereum - a secure decentralised generalised transaction ledger. eip-150 revision,” 2013. [Online]. Available: http://gavwood.com/paper.pdf. [Accessed: 16-Jan-2017]

[263] R. Macintosh, “The PhD Blog: Top 10 Hints For Understanding Your Ontology, Epistemology and Methodology,” *The PhD Blog*, 09-Jan-2017.

[Online]. Available: https://doctoralstudy.blogspot.com/2017/01/top-10-hints-for-understanding-your.html. [Accessed: 16-Oct-2018]

[264] The Basics of Philosophy, “Positivism,” 2008–2018. [Online]. Available: https://www.philosophybasics.com/branch_positivism.html. [Accessed: 17-Oct-2018]

[265] J. Dewey, *Logic the theory of inquiry*. 2013.

[266] A. Chakravartty, *Scientific ontology: Integrating naturalized metaphysics and voluntarist epistemology*. Oxford, UK : New York, NY: Oxford University Press, 2017.

[267] T. S. Kuhn and I. Hacking, *The structure of scientific revolutions*, Fourth edition. Chicago ; London: The University of Chicago Press, 2012.

[268] E. Phillips and D. S. Pugh, *How to get a PhD: A handbook for students and their supervisors*, 4th ed., revised and updated. Maidenhead: Open University Press, 2005.

[269] R. Bhaskar, *A realist theory of science*. Hassocks, Sussex : Atlantic Highlands, N.J: Harvester Press ; Humanities Press, 1978.

[270] J. Dudovskiy, “Interpretivism (interpretivist) Research Philosophy,” *Research-Methodology*, 2018. [Online]. Available: https://research-methodology.net/research-philosophy/interpretivism/. [Accessed: 23-Oct-2018]

[271] Web Centre for Social Research Methods, “Positivism and Post-Positivism,” 2018. [Online]. Available: http://www.socialresearchmethods.net/kb/positvsm.php. [Accessed: 22-Oct-2018]

[272] J.-F. Lyotard, *The postmodern condition: a report on knowledge*. Minneapolis: University of Minnesota Press, 1984.

[273] G. Aylesworth, “Postmodernism,” in *The Stanford Encyclopedia of Philosophy*, Spring 2015., E. N. Zalta, Ed. Metaphysics Research Lab, Stanford University, 2015 [Online]. Available: https://plato.stanford.edu/archives/spr2015/entries/postmodernism/. [Accessed: 11-Apr-2019]

[274] L. Cohen, L. Manion, and K. Morrison, *Research methods in education*, 5th ed. London ; New York: RoutledgeFalmer, 2000.

[275] E. Sober, *Core questions in philosophy: A text with readings*, 6th ed. Boston: Pearson Education, 2013.

Appendix A: Cryptography

Cryptography is the mathematics of information security [260], a field of study that investigates the confidentiality, integrity, authenticity and non-repudiation of data [261]. Below includes an explanation of some cryptographic tools - public-key cryptography, cryptographic hash functions and digital signatures, all of which are employed by blockchain technologies.

Public-key Cryptography

Data encryption is a process that produces an encoded message, known as ciphertext, by combining some text that must be kept secret, with a much shorter key. Decryption is the act of transforming ciphertext back into the original message [55].

Public-key cryptography (PKC) is a form of encryption that creates a public key, which is shared, widely, and a private key, which is known only to the owner [260]. The security of public-key cryptography is reliant upon the secrecy of the private key. Encryption is achieved using the public key and decryption using the private key [261]. Alice uses Bob's public key to encrypt a message that she wishes to send to him, privately. Only Bob can decrypt Alice's message since he is the only person who has the paired private key.

PKC systems rely on random numbers to generate public and private keys. Once generated, it is computationally infeasible to find the private key, given the public key alone. That is because they are one-way functions, a class of mathematical algorithms that are impractical to invert [261].

Cryptographic Hash Functions

Cryptographic hashes map arbitrary data to a unique fixed-size string. Alice can use that capability to ensure the integrity of any data she sends to Bob. She does so by computing a hash of her data, which she sends to Bob alongside the data itself. Once he receives both, Bob calculates the data's

cryptographic hash and checks that against the hash value Alice sent. If they match, Bob can be confident that the data is as Alice intended.

Cryptographic hash functions have the following properties:

1. **Deterministic**. The same data results in identical hashes.
2. **Fast**. For any data, it is quick to calculate the hash.
3. **One-way**. It is practically impossible to generate the data from its hash.
4. **No correlation**. A small change to a message will change the hash.
5. **Collision resistance**. It is computationally infeasible to find any two distinct inputs that hash to the same value [261].

However, there's another problem - how can Bob be sure that it was Alice who sent the data and its associated hash? Fortunately, cryptography provides a solution there. That is discussed next.

Digital Signatures

Hand-written signatures, which, before the Digital Revolution, served to identify, authorise and validate, are next to useless in cyberspace. Cryptography has developed techniques that offer identity authentication by allowing Alice to bind a digital signature to her messages. The general idea is that Alice produces a keypair, (s, v), of signing and verification keys. She publishes v, which anyone can read. Then, given a message, m, she can produce a signature σ (which takes the form of a number), such that anyone can check that σ is valid, thus proving the signing operation took place because σ relies upon a signers private key. That works by Alice executing a computational transform, so the final text she sends to Bob combines the original message with some secret information, her signature, which only she holds [260]. Bob then takes v, m and σ, and runs an algorithm that will only output true if, and only if, the signature was created honestly [29]. Furthermore, it is impossible to repudiate a digital signature, so Alice cannot deny that she was the sender.

Appendix B: Application Migration Costs

The smart contracts that are the basis of this thesis cost Ether to deploy. Appendix G of the Ethereum yellow paper details the calculations for determining the fee schedule of Ethereum transactions [262]. At the time of writing, the contracts have all been deployed to the Ethereum test network Rinkeby, using 'test Ether', which can be obtained via the Rinkeby faucet[60]. The deployments shown below demonstrate how much it would cost to deploy the same contracts to the main Ethereum network.

Enervator, Eneradmin and Enerchanger

Below are the costs of deployment of the seven smart contracts comprising the cryptocurrency Enervator and its two supporting applications, Eneradmin and Enerchanger.

Deploying 'Strings'

> transaction hash: 0xffac4f4b3122c0cf41a8aaac0acdb355264eef1597d49c1f8282bca0c566bd5b

> Blocks: 0 Seconds: 12

> contract address: 0xaCC92de46ef1Db4040438Eef78369CEb5e6604eb

> account: 0x8F03Ca885434522D695735A28d6A8A93b4390dA9

> balance: 7.590256574

> gas used: 815967

> gas price: 20 gwei

> value sent: 0 ETH

> total cost: 0.01631934 ETH

Deploying 'Exchanger'

> transaction hash: 0xef1f3f85a1f9e3c24c4d170b86e7300b3d0692e9e061de93b404e6cc6c93859d

> Blocks: 0 Seconds: 12

> contract address: 0x2484336c3a7812a3011ead2064ee0a7190B6F1a3

> account: 0x8F03Ca885434522D695735A28d6A8A93b4390dA9

> balance: 7.526155154

[60]Test Ether for the Ethereum Rinkeby blockchain are available via https://faucet.rinkeby.io/

> gas used: 3205071

> gas price: 20 gwei

> value sent: 0 ETH

> total cost: 0.06410142 ETH

Deploying 'Deposit'

> transaction hash: 0x263c936421491ae198024eed7a4c9089effb7e1f054d791a58db4d8b7887754c

> Blocks: 1 Seconds: 16

> contract address: 0x64c2D88F8298Dc4d8Ed95B6c8e12DEbf7d81f431

> account: 0x8F03Ca885434522D695735A28d6A8A93b4390dA9

> balance: 7.478304354

> gas used: 2392540

> gas price: 20 gwei

> value sent: 0 ETH

> total cost: 0.0478508 ETH

Deploying 'Forex'

> transaction hash: 0x149845e75b49cddb20348db7812410531b998dc6307dd0587641a980d8bc77ce

> Blocks: 0 Seconds: 12

> contract address: 0x2d6718857e21065Fec46bd29c729c1609Db4e2ac

> account: 0x8F03Ca885434522D695735A28d6A8A93b4390dA9

> balance: 7.466646174

> gas used: 582909

> gas price: 20 gwei

> value sent: 0 ETH

> total cost: 0.01165818 ETH

Deploying 'Buy'

> transaction hash: 0xc59f6a4cef759ce8f73f576bd249d508add031eacdc8a54474f389617c1b7394

> Blocks: 1 Seconds: 16

> contract address: 0x5e589FBB8BB4B0Df26a2A98b8F6ED873b74F5Fe7

> account: 0x8F03Ca885434522D695735A28d6A8A93b4390dA9

> balance: 7.432822954

> gas used: 1691161
> gas price: 20 gwei
> value sent: 0 ETH
> total cost: 0.03382322 ETH

Deploying 'EnervatorManager'

> transaction hash: 0x661862937b0944da82f14627dd9eea8dd5a54f96c3ecf77cb0682c7353d0cf2c
> Blocks: 0 Seconds: 12
> contract address: 0x639AaB41667FFB0Dffb9FA90201470361D6133E7
> account: 0x8F03Ca885434522D695735A28d6A8A93b4390dA9
> balance: 7.358480754
> gas used: 3717110
> gas price: 20 gwei
> value sent: 0 ETH
> total cost: 0.0743422 ETH

Deploying 'Enervator'

> transaction hash: 0x60ed54a82d1f8cfe167a4dca3172cef7965cd97aa4959398935e44a4370e6ec6
> Blocks: 1 Seconds: 16
> contract address: 0x5483b2996BBa07330E188Fe10BB101d4c1Ac8530
> account: 0x8F03Ca885434522D695735A28d6A8A93b4390dA9
> balance: 7.284716994
> gas used: 3688188
> gas price: 20 gwei
> value sent: 0 ETH
> total cost: 0.07376376 ETH

Saving migration to chain

> Total cost: 0.32185892 ETH

Provenator

Below are the costs of deployment of the five smart contracts comprising Provenator.

Deploying 'Strings'

> transaction hash:
0xf31b1149d85caf1d83bd40d2a2b958e21db7753b3299f075c93f42019b3f125a

> Blocks: 1 Seconds: 16

> contract address: 0x33288d818024cf758Ce964017cFa352fc01FDfd3

> account: 0x8F03Ca885434522D695735A28d6A8A93b4390dA9

> balance: 7.251076254

> gas used: 886777

> gas price: 20 gwei

> value sent: 0 ETH

> total cost: 0.01773554 ETH

Deploying 'PremisAgent'

> transaction hash:
0x4922c6759f86a400e679463f85638405625445ddb9408ee9a3f88ef6159c35be

> Blocks: 0 Seconds: 12

> contract address: 0x8AF724be59D960ad5DEbbB329aCD51fB4031d4eE

> account: 0x8F03Ca885434522D695735A28d6A8A93b4390dA9

> balance: 7.184621094

> gas used: 3322758

> gas price: 20 gwei

> value sent: 0 ETH

> total cost: 0.06645516 ETH

Deploying 'PremisEvent'

> transaction hash:
0x830994fb7ac65691cabccbb06811d0a412bab79f383a3bb2c3d20ae46d7a93b4

> Blocks: 1 Seconds: 16

> contract address: 0x5c33249064D7D9BC24f64ffC2BA13b4f7FdB7554

> account: 0x8F03Ca885434522D695735A28d6A8A93b4390dA9

> balance: 7.144428594

> gas used: 2009625

> gas price: 20 gwei

> value sent: 0 ETH

> total cost: 0.0401925 ETH

```
Deploying 'PremisObject'
------------------------
> transaction hash:
0x3ebf597281dfa659c815fea71ac9495961085066034312cc8e3874147959aed8
> Blocks: 1          Seconds: 16
> contract address:    0xF0954cd622829578C5bE3130fbf573AE5658e496
> account:           0x8F03Ca885434522D695735A28d6A8A93b4390dA9
> balance:           7.049811914
> gas used:          4730834
> gas price:         20 gwei
> value sent:        0 ETH
> total cost:        0.09461668 ETH

Deploying 'PremisRights'
------------------------
> transaction hash:
0x9a9f107637155ea832aefde0f540b3b834fbbb07ac3a10e1eee36203338c8a79
> Blocks: 0          Seconds: 12
> contract address:    0x37567FE1F9C385c97D4b4Ec29DEC7978cA7C3de1
> account:           0x8F03Ca885434522D695735A28d6A8A93b4390dA9
> balance:           6.978652194
> gas used:          3557986
> gas price:         20 gwei
> value sent:        0 ETH
> total cost:        0.07115972 ETH

Saving migration to chain
-------------------------
> Total cost:         0.2901596 ETH
```

ReportAid

Below are the costs of deployment of the fourteen smart contracts comprising ReportAid.

```
Deploying 'Strings'
-------------------
> transaction hash:
0xe713ceb05f3ef29b61e5cf6e36f53e8b133155a4ca2d92a305eb35d681f32588
> Blocks: 0          Seconds: 0
```

> contract address: 0xB355862B3cC0Ea3b4E0622c7B7Ef190A7EAB252e
> account: 0xd400515d7Bb28Ed05d027a3DA14928CEDCeE0DAb
> balance: 83.3202776
> gas used: 824320
> gas price: 20 gwei
> value sent: 0 ETH
> total cost: 0.0164864 ETH

Deploying 'IATIOrgs'

> transaction hash:
0xdc8374a3a9fafd0b7c290390a00deb3a178099930bcc8cab9a77d65d8b5837c6
> Blocks: 0 Seconds: 0
> contract address: 0x38172AD1d09e3e3815c2962B8122a1Cc55C6aA8d
> account: 0xd400515d7Bb28Ed05d027a3DA14928CEDCeE0DAb
> balance: 83.29978922
> gas used: 1024419
> gas price: 20 gwei
> value sent: 0 ETH
> total cost: 0.02048838 ETH

Deploying 'IATIOrganisations'

> transaction hash:
0x6b3abbe04e25e07c7bdf148572e97655b48be6667352195590e7cf09a9b8acc6
> Blocks: 0 Seconds: 0
> contract address: 0xa17b6586c5E254039Ae83C9F46c71a99682e63fb
> account: 0xd400515d7Bb28Ed05d027a3DA14928CEDCeE0DAb
> balance: 83.28507682
> gas used: 735620
> gas price: 20 gwei
> value sent: 0 ETH
> total cost: 0.0147124 ETH

Deploying 'IATIOrganisation'

> transaction hash:
0x8da19311fbff32d01be487c01c4ffd9489429e62e504ed58d5e9ff406268c104

> Blocks: 0 Seconds: 0

> contract address: 0xd539795974B6b279fb7ce2ce9608d7fBC524FC7D

> account: 0xd400515d7Bb28Ed05d027a3DA14928CEDCeE0DAb

> balance: 83.24956372

> gas used: 1775655

> gas price: 20 gwei

> value sent: 0 ETH

> total cost: 0.0355131 ETH

Deploying 'IATIOrganisationDocs'

> transaction hash: 0x7384eae6c94deb94fca105ad0bbff74365f5c08bb4b41f0d11bfa3058c7737ea

> Blocks: 0 Seconds: 0

> contract address: 0xf647cD62d16673a40c99A98c9C0444868F6E5c02

> account: 0xd400515d7Bb28Ed05d027a3DA14928CEDCeE0DAb

> balance: 83.19451548

> gas used: 2752412

> gas price: 20 gwei

> value sent: 0 ETH

> total cost: 0.05504824 ETH

Deploying 'IATIBudgets'

> transaction hash: 0xc036bf768dddd1fb9241508e218029eb381a19e15ec6ad96fde8a257fc03d6c0

> Blocks: 0 Seconds: 0

> contract address: 0x2329539D2A9F54F7bc86e8f9c425c21254C277E5

> account: 0xd400515d7Bb28Ed05d027a3DA14928CEDCeE0DAb

> balance: 83.15504744

> gas used: 1973402

> gas price: 20 gwei

> value sent: 0 ETH

> total cost: 0.03946804 ETH

Deploying 'IATIActivities'

> transaction hash:
0x6d01051ab4b915ef3a7a45e088745eff32cc7f25447f9a9669247541cc141d76

> Blocks: 0 Seconds: 0

> Blocks: 0 Seconds: 0

> contract address: 0x67ed281882baFE20044050B2AF6E5466dCeC1dca

> account: 0xd400515d7Bb28Ed05d027a3DA14928CEDCeE0DAb

> balance: 83.0099732

> gas used: 813473

> gas price: 20 gwei

> value sent: 0 ETH

> total cost: 0.01626946 ETH

Deploying 'IATIOrganisationBudgets'

> transaction hash:
0x370d2a07f136afec34e7cfd2e9feb26ab4ef469e9ee8af87bdfc53b3bee2ed0f

> Blocks: 0 Seconds: 0

> contract address: 0xb2E10F33ACc31B0758e5f048eB6390C1Eb0B125D

> account: 0xd400515d7Bb28Ed05d027a3DA14928CEDCeE0DAb

> balance: 83.0099732

> gas used: 1243298

> gas price: 20 gwei

> value sent: 0 ETH

> total cost: 0.02486596 ETH

Deploying 'IATIOrganisationExpenditure'

> transaction hash:
0x0d9443dd7cdcc4d6cba919dccc1b643fe444fda17ac703e11d28e81c2ed193f5

> Blocks: 0 Seconds: 0

> contract address: 0xC80C1F9Bd982e4dF93069a646522B6167b62cb1d

> account: 0xd400515d7Bb28Ed05d027a3DA14928CEDCeE0DAb

> balance: 83.0099732

> gas used: 1243554

> gas price: 20 gwei

> value sent: 0 ETH

> total cost: 0.02487108 ETH

Deploying 'IATIOrganisationRecipientBudgets'

```
-------------------------------------------
> transaction hash:
0x34b8a5debbd4b52718205bb6f9da0072bc054e91d9d98221b61892eec3bcdd27
> Blocks: 0            Seconds: 0
> contract address:    0x9089ea8CA4d522AFddd55e0Ae92d99C6d398d92D
> account:             0xd400515d7Bb28Ed05d027a3DA14928CEDCeE0DAb
> balance:             83.0099732
> gas used:            1317817
> gas price:           20 gwei
> value sent:          0 ETH
> total cost:          0.02635634 ETH


Deploying 'IATIOrganisationRegionBudgets'
-----------------------------------------
> transaction hash:
0x36b8b49759854c3ddea44bd6c6d0cdf3337f3aec837953a8b9781428f654dd2d
> Blocks: 0            Seconds: 0
> contract address:    0x94206500f3731712d2e924b58feb913E3c7f0bFf
> account:             0xd400515d7Bb28Ed05d027a3DA14928CEDCeE0DAb
> balance:             83.0099732
> gas used:            1317817
> gas price:           20 gwei
> value sent:          0 ETH
> total cost:          0.02635634 ETH


Deploying 'IATIOrganisationCountryBudgets'
------------------------------------------
> transaction hash:
0x143daace0a49ecaa1c729eaeab52a3271138dc417886ef360a925653fbe0d48f
> Blocks: 0            Seconds: 0
> contract address:    0x7Dc4877c92Cc35e0EbdCfDc8EFb65cFf19140Db7
> account:             0xd400515d7Bb28Ed05d027a3DA14928CEDCeE0DAb
> balance:             83.0099732
> gas used:            1317753
> gas price:           20 gwei
> value sent:          0 ETH
> total cost:          0.02635506 ETH


Deploying 'IATIActivity'
```

```
----------------------
> transaction hash:
0x6b3c194fa80f6385a9883ba5716933919cfbdc96ed1d3dd3fe5da8b7759d426f
> Blocks: 0            Seconds: 0
> contract address:    0xafFC46ffc9B2977AF462E7f22A21B7337d4B7d01
> account:             0xd400515d7Bb28Ed05d027a3DA14928CEDCeE0DAb
> balance:             82.9357198
> gas used:            3712670
> gas price:           20 gwei
> value sent:          0 ETH
> total cost:          0.0742534 ETH


Deploying 'IATIActivityDates'
-----------------------------
> transaction hash:
0x7a8df684e0816bd9cfbb5c7b3ecfcfadb78c7901af28781e82f7405e7e5763e0
> Blocks: 0            Seconds: 0
> contract address:    0x47Bb9194f9932c837A1C6bb9190FD4E5dA5Fc94a
> account:             0xd400515d7Bb28Ed05d027a3DA14928CEDCeE0DAb
> balance:             82.9022371
> gas used:            1674135
> gas price:           20 gwei
> value sent:          0 ETH
> total cost:          0.0334827 ETH

Saving migration to chain
-------------------------
> Total cost:          0.4345269 ETH
```

Appendix C: Research Philosophy

This is a general introduction to research philosophy. It provides some background to the methodological assumptions made during this thesis.

Ontology, Epistemology and Axiology

A set of assumptions informs any intellectual endeavour [263]. Those assumptions have a profound influence on research analysis because they help define the discoveries made [196]. Ontological assumptions include those made about the nature of reality. Epistemological assumptions are concerned with how we obtain knowledge which reveals that reality. Axiological assumptions influence the extent to which our inherent values influence research. Hence, ontology is the branch of metaphysical philosophy that examines the essential qualities of existence. Epistemology is the theory of knowledge; it attempts to justify the beliefs that reveal ontological truths [196], and axiology is the study of the human values and valuation [25].

An objective ontology believes in one actual reality that is independent of human consciousness [191], whereas a subjective ontology believes that reality is a factor of our perception [194]. Epistemologically, the objective philosophies rely on observable facts and phenomenon, whereas those that are subjective offer opinions of observed events. Axiologically, the objective philosophies believe in value-free detachment, whereas the subjective philosophies suggest that inherent values are important [194]. Below is a summary of some objective and subjective research philosophies.

Positivism

Positivism is the objective belief that the world is deterministic because it is explained via a set of static parameters. Positivists claim that science provides the only authentic knowledge since it positively affirms theories based on observable and measurable evidence [264]. Hence, the philosophy relies on that which is posited, so an emphasis is given to empirical

methods designed to yield a quantitative reality uninfluenced by human interpretation [194].

A positivist researcher attempts to detach themselves from their research so as not to exact any influence over their quantifiable results. They develop a hypothesis via existing theories, which are used to create axiomatic generalisations that are confirmed and tested through measurable facts [194].

Pragmatism

Pragmatism is the view that the goal of science is not to understand the true nature of things, but rather, it is to produce useful knowledge through practical activities [265]. It is the philosophical belief that, due to different means of interpretation, there are multiple realities, so no single point of view can reveal the world in its entirety [194]. Kuhn argued that science undergoes cyclical patterns, based on historical context, which defines scientific terminology by strict boundaries, determined by what is considered normative for a given period [266]. Hence, the science of one age is supplanted by that of another, through a series of "paradigm shifts" [267]. For example, Einstein's relativity has replaced Newtonian physics, and the term *mass* meant something different to Einstein than it did to Newton. Kuhn believed, therefore, that economic and political factors reshape scientific research into finite sets of historically contingent relations between ideas about the world [266]. The result is that, rather than stating hard facts about what exists, the researcher is only capable of making scientific claims that are grounded in the ideas of the time. Furthermore, the terms of our experiences limit those claims because they are informed only by our observations and the methods by which we have learned to solve problems, "every act of observation we make is a function of what we have seen or otherwise experienced in the past. All scientific work of an experimental or exploratory nature starts with some expectation about the outcome" [268].

A pragmatist strives to reconcile both objectivism and subjectivism by considering theories in terms of their practical consequences and the

contexts in which they are produced [194]. Therefore, a pragmatist researcher may adopt different philosophical stances to tackle a research problem, since their view that there may be multiple realities is only reconcilable if they consider many different approaches to understanding.

Critical Realism

Realism is the idea that we can gain reliable knowledge of a reality that is independent of human consciousness [191]. Critical realism, developed in the late 20th Century by the philosopher Roy Bhaskar [269], is a form of realism which concludes an independent reality is **not** directly accessible through observation, because our senses deceive us. Rather than revealing the real world, all our senses reveal are mere sensations that are subjective manifestations of the real world.

A critical realist believes there are two steps to understanding reality; the first step involves the events we experience. The second step is the mental agility required to step back through those experiences and thereby, understand them. Therefore, critical realists believe our reasoning is qualitatively 'retroductive' because it involves inductive reprocessing of sensations. Furthermore, critical realists are epistemologically and axiologically relativist because they insist knowledge is a result of social conditioning relative to a particular time [194]. Bhaskar believed that we can only understand society through an examination of social structures, which means that, although a critical realist researcher is much less objectivist than a positivist, they must seek to remove subjective bias by striving to achieve an awareness of the ways in which their socio-cultural background and experiences influence their research. Hence, critical realism is stratified because it is epistemologically subjective but ontologically objective.

Interpretivism

Interpretivism acknowledges the role of the researcher; it accepts their normative values, and that subjectivity introduces an inherent bias [270]. It is phenomenological (from the Greek *phainómenon*, meaning *that which*

appears, and *lógos*, meaning *study*), because it imparts relevance to the researcher's conscious experience.

Interpretivism is dependent upon a postpositivism epistemology. Postpositivism emerged during the latter part of the 20th Century when it embarked on a wholesale rejection of the positivists' belief in a single, overarching reality [196]. Instead, postpositivists believe that different perspectives offer many realities [271]. They contend the objectivist view that there is external meaning independent of consciousness. For example, "The United States of America" means one thing to Donald Trump, but something else entirely to a twelve-year-old Central-American refugee held in an immigration camp in Texas. In other words, our cultural experiences bias our view of reality.

Many postpositivists are constructivists who believe that we construct our world view through personal perception, which must be imperfect because observation is fallible [271]. Indeed, postpositivism argues that the goal should be an interpretation, rather than absolute truth [196]. Furthermore, because they believe it is impossible to know anything with any certainty, postpositivism rejects the relativist idea of the incommensurability of different perspectives, whereby people with different cultural experiences can never understand one another; after all, to a Native American, Donald Trump is an immigrant, too. Hence, if that twelve-year-old refugee was allowed entry into the United States and given the right opportunities, she might one day have a daughter who becomes President.

An interpretivist researcher suggests that different perspectives offer multiple views of reality, so they take an explicitly subjectivist standpoint, which attempts to create a rich understanding of society. Axiologically, an interprevist recognises that their values play an essential role in their research processes [194].

Postmodernism

Postmodernism first came to being in 1979, with the publication of The Postmodern Condition by Jean-François Lyotardis [272]. It is, "a set of critical, strategic and rhetorical practices employing concepts such as

difference, repetition, the trace, the simulacrum, and hyperreality to destabilise other concepts" [273]. Hence, it is a subjective philosophy that seeks to subvert social norms, thus giving voice to alternative viewpoints.

In rejecting objective positivism, postmodernists go even further than interpretivism. They believe any sense of order is only realisable through our language because, beyond the world of language, there is chaos. Hence, a postmodernist believes there is no abstract way of determining the correct way of understanding the world; instead, at any given time, what is generally considered to be correct are social conditions determined by the power relations and the ideologies that dominate. Furthermore, this does not mean that the dominant ways of thinking are right! Merely, they are seen as such at that time because other perspectives, which may be just as valuable and have the power to create alternative worlds and truths, have been suppressed [194].

Hence, a postmodernist researcher deconstructs societal norms by challenging accepted perception and emphasising excluded realities. They give recognition to the power relations between the researcher and the topic of interest, which shapes the knowledge formed as part of the research process [194]. Indeed, power relations are fundamental to the postmodernist researcher, so they must illicit their values during their research and include radically reflexive responses to their findings.

Research Paradigms

In their 1979 book, *Sociological Paradigms and Organisational Analysis: Elements of the Sociology of Corporate Life*, Burrell and Morgan define a paradigm as a set of philosophical assumptions that influence research [198]. Such assumptions have implications because they define how research is conducted [274]. Figure C.1, below, attempts to quantify research paradigms, whereby the researcher's approach is dependent upon the degree of their subjectivism against the degree of their social regulation [194]. The top half of Figure C.1 shows a researcher who believes in conflict. Their radical perspective sees deprivation. It advocates change and introduces constructive chaos because it challenges the

dominant hegemony. By contrast, the lower half shows a researcher who has a regulation perspective that is inherently conservative. It advocates the status quo, order, consensus, cohesion and solidarity.

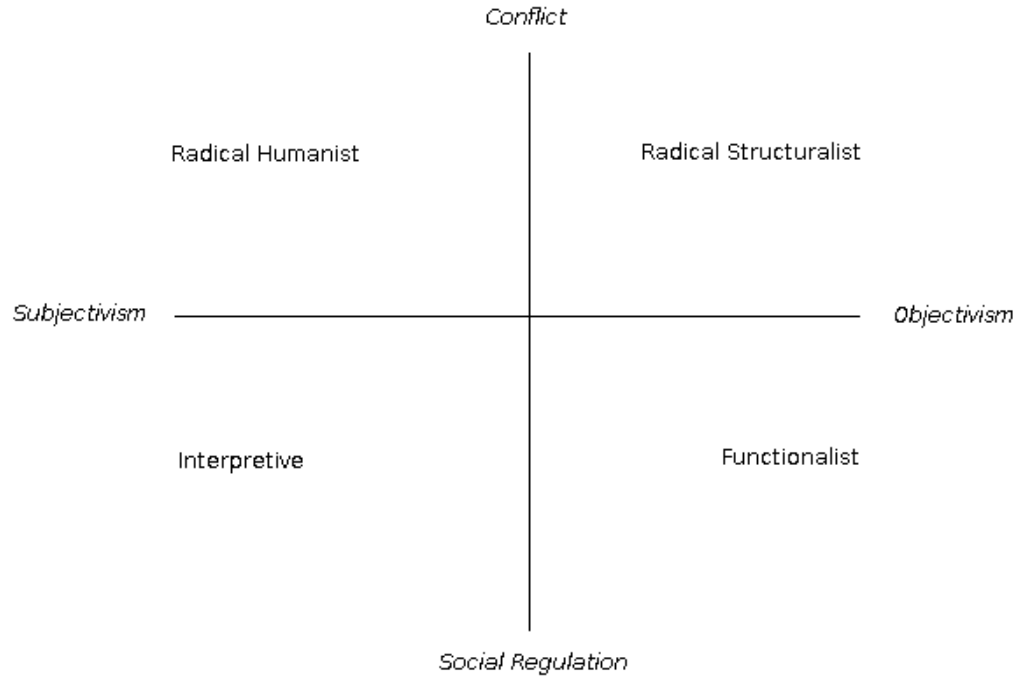


Figure C.1: The Four paradigms of research [198]

The radical structuralist paradigm approaches research from a critical realist perspective by attempting to understand structural patterns, such as hierarchies, and the extent to which they dominate and oppress [194]. The radical humanist paradigm is also concerned with power relations, but the focus is more postmodern, whereby it looks at the effects of social construction and language. The functionalist paradigm is on the objectivist and regulatory dimensions of research, which is likely to fit the positivist philosophy because that believes in rational explanations that lie within existing regulating structures. The interpretive paradigm focuses on multiple subjective realities that are influenced by power relations and how humans attempt to make sense of their world.

Research Approaches

The researcher may use different forms of reasoning during research, including deductive, inductive, abductive or a combined inductive-deductive approach [274]. Deduction reaches conclusions via a logical progression from the general to the particular:

x is derived from y, only when x is logically consequent from y.

Deduction is a form of systematic reasoning that is the result of Aristotle's syllogism:

```
All planets orbit the sun;
The earth is a planet;
Therefore the earth orbits the sun.
```

Around the turn of the 17th century, Francis Bacon began to argue for an inductive means of reasoning, which, rather than providing definitive logical proof, reaches a general conclusion by emphasising observation of particular circumstances [274]:

x is inferred from y, but x is not necessarily a logical consequence of y.

In other words, *y* might give sufficient reason to accept *x*, but it does not ensure *x*.

A combination of Aristotle and Bacon's approaches moves inductively from observation to hypotheses, whereby conclusions are verified by deducing implications.

In the 19th Century, Charles Sanders Peirce introduced the idea of pragmatic abductive reasoning, which seeks to arrive at the most plausible explanation from a set of observations [275]. Here, a hypothesis is merely a 'guess', which is made more robust through logical verification:

y as an explanation of x, whereby y is abduced from the consequence x.

Abduction is a formal fallacy that is equivalent to a converse error, which takes a fact and incorrectly draws inferences for situations that may have many explanations. For example, "My thesis did not print. Therefore, the printer must be broken". However, there could be many reasons why my thesis did not print. Despite this, abduction remains useful because it

allows us to hypothesise against our observations and arrive at explanations that eventually lead to more reasonable solutions. For example, having investigated the supposed broken printer, I discovered its power button and turned it on. The result is you may well be reading a hard copy of this thesis.

Appendix D: The AWARE XML

Below is the source XML modelled in Chapter 9.


```
<?xml version="1.0" encoding="UTF-8"?>
<iati-activities xmlns:iati-extra="http://datastore.iatistandard.org/ns">
  <iati-activity last-updated-datetime="2019-10-11T13:39:21"
xml:lang="en" default-currency="EUR" humanitarian="0" hierarchy="1"
generated-datetime="2019-10-11T12:53:35" version="2.02">
    <iati-identifier>XI-IATI-EC_DEVCO-2014/37785/0</iati-identifier>
    <reporting-org ref="XI-IATI-EC_DEVCO" type="15">
      <narrative xml:lang="en">European Commission - Development and
Cooperation-EuropeAid</narrative>
    </reporting-org>
    <title>
      <narrative xml:lang="en">A West African Response to Ebola
(AWARE)</narrative>
    </title>
    <description type="1">
      <narrative>The overall obj: to mitigate negative effects of the Ebola
outbreak&contribute to the recovery of the most affected countries in
West-Africa. The specific obj: to strengthen health systems to improve
access to quality PHC, resilience&awareness.</narrative>
    </description>
    <participating-org ref="XI-IATI-EC_DEVCO" role="1" type="15"
activity-id="XI-IATI-EC_DEVCO-2014/37785/0">
      <narrative xml:lang="en">European Commission - Directorate-General
for International Cooperation and Development (DEVCO)</narrative>
    </participating-org>
    <participating-org ref="XI-IATI-EC_DEVCO" role="3" type="15"
activity-id="XI-IATI-EC_DEVCO-2014/37785/0">
      <narrative xml:lang="en">European Commission - Directorate-General
for International Cooperation and Development (DEVCO)</narrative>
```

</participating-org>
<participating-org ref="20000" role="2" activity-id="XI-IATI-EC_DEVCO-2014/37785/0">
<narrative xml:lang="en">NON-GOVERNMENTAL ORGANISATIONS (NGOs) AND CIVIL SOCIETY</narrative>
</participating-org>
<participating-org ref="N/A" role="4" type="N/A" activity-id="XI-IATI-EC_DEVCO-2014/37785/0">
<narrative xml:lang="en">NON-GOVERNMENTAL ORGANISATIONS (NGOs) AND CIVIL SOCIETY</narrative>
</participating-org>
<activity-status code="2"/>
<activity-date iso-date="2015-12-15" type="1">
<narrative xml:lang="en">Planned Start: 15-DEC-15</narrative>
</activity-date>
<activity-date iso-date="2015-03-09" type="2">
<narrative xml:lang="en">Actual Start: 09-MAR-15</narrative>
</activity-date>
<activity-date iso-date="2018-11-27" type="3">
<narrative xml:lang="en">Planned End: 27-NOV-18</narrative>
</activity-date>
<activity-date iso-date="2050-12-31" type="4">
<narrative xml:lang="en">Actual End: 31-DEC-50</narrative>
</activity-date>
<contact-info>
<organisation>
<narrative xml:lang="en">Delegation of the European Union to Nigeria</narrative>
</organisation>
<department>
<narrative xml:lang="en">Delegation of the European Union to Nigeria</narrative>

```
      </department>
      <telephone>+234 9-4617800</telephone>
      <email>delegation-nigeria@ec.europa.eu</email>

<website>http://eeas.europa.eu/delegations/nigeria/index_en.htm</website>
    </contact-info>
    <activity-scope code="1"/>
    <recipient-region code="289" vocabulary="1">
      <narrative xml:lang="en">South of Sahara, regional</narrative>
    </recipient-region>
    <sector code="12250" vocabulary="1">
      <narrative xml:lang="en">Infectious disease control</narrative>
    </sector>
    <policy-marker code="01" significance="0" vocabulary="DAC">
      <narrative xml:lang="en">Gender Equality</narrative>
    </policy-marker>
    <policy-marker code="02" significance="0" vocabulary="DAC">
      <narrative xml:lang="en">Aid to Environment</narrative>
    </policy-marker>
    <policy-marker code="03" significance="0" vocabulary="DAC">
      <narrative xml:lang="en">Participatory
Development/Good</narrative>
    </policy-marker>
    <policy-marker code="04" significance="0" vocabulary="DAC">
      <narrative xml:lang="en">Trade Development</narrative>
    </policy-marker>
    <policy-marker code="05" significance="0" vocabulary="DAC">
      <narrative xml:lang="en">Aid Targeting the Objectives of the
Convention on Biological Diversity</narrative>
    </policy-marker>
    <policy-marker code="06" significance="0" vocabulary="DAC">
```

<narrative xml:lang="en">Aid Targeting the Objectives of the Framework Convention on Climate Change - Mitigation</narrative>
</policy-marker>
<policy-marker code="07" significance="0" vocabulary="DAC">
<narrative xml:lang="en">Aid Targeting the Objectives of the Framework Convention on Climate Change - Adaptation</narrative>
</policy-marker>
<policy-marker code="08" significance="0" vocabulary="DAC">
<narrative xml:lang="en">Aid Targeting the Objectives of the Convention to Combat Desertification</narrative>
</policy-marker>
<policy-marker code="09" significance="0" vocabulary="DAC">
<narrative xml:lang="en">Contributions To Reproductive, Maternal, Newborn and Child Health¿</narrative>
</policy-marker>
<collaboration-type code="1"/>
<default-flow-type code="10"/>
<default-finance-type code="110"/>
<default-aid-type code="D02"/>
<default-tied-status code="5"/>
<budget type="1" status="2">
<period-start iso-date="2020-01-01"/>
<period-end iso-date="2020-12-31"/>
<value currency="EUR" value-date="2019-10-11">0</value>
</budget>
<budget type="1" status="2">
<period-start iso-date="2019-01-01"/>
<period-end iso-date="2019-12-31"/>
<value currency="EUR" value-date="2019-10-11">0</value>
</budget>
<planned-disbursement type="1">
<period-start iso-date="20191900-01-01"/>

```
      <period-end iso-date="2017-12-01"/>
      <value currency="EUR" value-date="2019-10-11">150000</value>
      <provider-org provider-activity-id="XI-IATI-EC_DEVCO-2014/37785/0"
type="15">
        <narrative>XI-IATI-EC_DEVCO</narrative>
      </provider-org>
      <receiver-org receiver-activity-id="XI-IATI-EC_DEVCO-2014/37785/0"/
>
    </planned-disbursement>
    <planned-disbursement type="1">
      <period-start iso-date="20191900-01-01"/>
      <period-end iso-date="2017-12-01"/>
      <value currency="EUR" value-date="2019-10-11">150000</value>
      <provider-org provider-activity-id="XI-IATI-EC_DEVCO-2014/37785/0"
type="15">
        <narrative>XI-IATI-EC_DEVCO</narrative>
      </provider-org>
      <receiver-org receiver-activity-id="XI-IATI-EC_DEVCO-2014/37785/0"/
>
    </planned-disbursement>
    <planned-disbursement type="1">
      <period-start iso-date="20191900-01-01"/>
      <period-end iso-date="2017-12-01"/>
      <value currency="EUR" value-date="2019-10-11">150000</value>
      <provider-org provider-activity-id="XI-IATI-EC_DEVCO-2014/37785/0"
type="15">
        <narrative>XI-IATI-EC_DEVCO</narrative>
      </provider-org>
      <receiver-org receiver-activity-id="XI-IATI-EC_DEVCO-2014/37785/0"/
>
    </planned-disbursement>
    <planned-disbursement type="1">
```

```
      <period-start iso-date="20191900-01-01"/>
      <period-end iso-date="2017-12-01"/>
      <value currency="EUR" value-date="2019-10-11">150000</value>
      <provider-org provider-activity-id="XI-IATI-EC_DEVCO-2014/37785/0"
type="15">
        <narrative>XI-IATI-EC_DEVCO</narrative>
      </provider-org>
      <receiver-org receiver-activity-id="XI-IATI-EC_DEVCO-2014/37785/0"/
>
    </planned-disbursement>
    <capital-spend percentage="0"/>
    <transaction ref="XI-IATI-EC_DEVCO-2014/37785/0/0"
humanitarian="0">
      <transaction-type code="2"/>
      <transaction-date iso-date="2014-12-11"/>
      <value currency="EUR" value-date="2019-10-11">28000000</value>
      <provider-org ref="XI-IATI-EC_DEVCO" provider-activity-id="XI-IATI-
EC_DEVCO-2014/37785/0" type="15"/>
      <receiver-org>
        <narrative xml:lang="en"/>
      </receiver-org>
      <disbursement-channel code="2"/>
      <sector vocabulary="1" code="12250">
        <narrative xml:lang="en">Infectious disease control</narrative>
      </sector>
      <recipient-region code="289" vocabulary="1">
        <narrative xml:lang="en">South of Sahara, regional</narrative>
      </recipient-region>
      <tied-status code="5"/>
    </transaction>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/358-184" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/358-191" type="2"/>
```

```
    <related-activity ref="XI-IATI-EC_DEVCO-2015/358-224" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/358-227" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/358-232" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/359-047" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/363-727" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/365-129" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/369-334" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/370-891" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/370-908" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/371-138" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/371-573" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/371-640" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/371-653" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/371-655" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/371-880" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2015/372-110" type="2"/>
    <related-activity ref="XI-IATI-EC_DEVCO-2018/398-579" type="2"/>
  </iati-activity>
</iati-activities>
```