2018

Identifying and Scoping Context-Specific Use Cases For Blockchain-Enabled Systems in the Wild.

Fiona Delaney
Technological University Dublin

Identifying and scoping context-specific use cases for blockchain-enabled systems in the wild.

Fiona Delaney

D12125908

A dissertation submitted in partial fulfilment of the requirements of

Dublin Institute of Technology for the degree of

M.Sc. in Computing (Advanced Software Development)

2018

I certify that this dissertation which I now submit for examination for the award of MSc in Computing (Knowledge Management), is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the test of my work.

This dissertation was prepared according to the regulations for postgraduate study of the Dublin Institute of Technology and has not been submitted in whole or part for an award in any other Institute or University.

The work reported on in this dissertation conforms to the principles and requirements of the Institute's guidelines for ethics in research.

Signed: **Fiona Delaney**____________________________

Date: **January 3rd 2018**__________________________

ABSTRACT

Advances in technology often provide a catalyst for digital innovation. Arising from the global banking crisis at the end of the first decade of the 21st Century, decentralised and distributed systems have seen a surge in growth and interest. Blockchain technology, the foundation of the decentralised virtual currency Bitcoin, is one such catalyst.

The main component of a blockchain, is its public record of verified, timestamped transactions maintained in an append-only, chain-like, data structure. This record is replicated across *n*-nodes in a network of co-operating participants. This distribution offers a public proof of transactions verified in the past.

Beyond tokens and virtual currency, real-world use cases for blockchain technology are in need of research and development. The challenge in this proof-of-concept research is to identify an orchestration model of innovation that leads to the successful development of software artefacts that utilise blockchain technology. These artefacts must maximise the potential of the technology and enhance the real-world business application.

An original two phase orchestration model is defined. The model includes both a discovery and implementation phase and implements state-of-the-art process innovation frameworks: Capability Maturity Modelling, Business Process Redesign, Open Innovation and Distributed Digital Innovation.

The model succeeds in its aim to generate feasible problem-solution design pairings to be implemented as blockchain enabled software systems. Three systems are developed: an internal supply-chain management system, a crowd-source sponsorship model for individual players on a team and a proof-of-origin smart tag system. The contribution is to have defined an innovation model through which context-specific blockchain use-cases can be identified and scoped in the wild.

Key words: *digital innovation, blockchain-enabled systems.*

ACKNOWLEDGEMENTS

Thanks to everyone at Bohemians FC who took part in this research, in particular Deirdre Clifford, Ian Morris and Conor Emerson. Much appreciation is due to Supervisor Dr. Sean O'Leary, whose patience and insights were warmly received throughout. Finally, thank you to my family Eamon, Ciaran and Alexander whose good-humoured support and encouragement are constant.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1. INTRODUCTION

1.1 Background

Advances in technology often provide the catalyst for digital process re-design and engineering. Arising from the global banking crisis at the end of the first decade of the 21^{st} Century, decentralised and distributed systems have seen a surge in growth and interest (Nakamoto, 2009). Blockchain technology, the foundation of the decentralised virtual currency Bitcoin, is one such catalyst.

The main component of a blockchain, is its public record of verified, timestamped transactions maintained in an append-only, chain-like, data structure. This record is replicated across *n*-nodes in a network of co-operating participants. This distribution offers a public proof of transactions verified in the past. The nodes must reach consensus about valid block-ordering by solving cryptographic puzzles and by following 'the longest chain rule'. This rule states that where two nodes confirm blocks simultaneously (causing a temporary fork in the chain) the fork with the subsequent longest chain is deemed to be correct. All nodes (including the forked chain) shall synchronise with the longer chain. (Bitcoin, 2009; Multichain, 2014; Ethereum, 2015; Tendermint, 2016).

There are a number of blockchain implementations considered here including: Multichain, an Open Source fork from Bitcoin core enabling the simple implementation of private blockchains; Ethereum (current version Byzantium), a public blockchain platform which requires code written in specific languages (e.g. Solidity, Serpent or LLL) to compile on the Ethereum Virtual Machine and Tendermint core, a private blockchain implementation which uses an Application Block Chain Interface (ABCI) to access the Tendermint distributed state machine.

Two distributed, peer-to-peer approaches to generating cryptographic solutions to secure and valid distributed ledgers are examined: blockchain and hashgraph. To describe the newcomer first, Hashgraph is a java-based application, which uses a hash-graph data structure as a distributed state machine to store information across multiple nodes. Blockchain, the more familiar solution, utilises a chain-like data structure to cryptographically determine and secure an append-only, time series of stored data.

1.2 Research Project/problem

Blockchain technology is a relatively new research field and according to Yli-Huumo et al, (2016) there are three main gaps in the research field: usability from both end-user and developer perspectives, empirical research in performance metrics and network utility, and scoping potential business uses cases.

Scoping real world commercial use cases for blockchain-enabled DApps[1] is a current trend in a wide range of business contexts[2]. Some examples include: Corda (2015) R3's global banking research initiative; VeChain (2017) a Price Waterhouse Cooper side-project introducing blockchain-based product traceability and supply chain management and Provenance (2016) a consumer-facing quality assurance application.

There is ongoing development of brand new markets facilitated by blockchain and what has been termed a crypto-economic ecosystem[3]. Some popular and infamous examples include: Cryptokitties (Zen, 2017), a kitten-breeding game on Ethereum and the ill-fated Ethereum venture: 'The DAO' (2015). In blockchain research, the lack of fully scoped and implemented business use cases, either hypothetical, virtual or in the wild, is noted (CeADAR, 2015; Yli-Huumo et al., 2016).

---

[1] DApp - Decentralised Application. A DApp has backend code running on a peer-to-peer network, not on centralised servers, often implementing smart contracts, or transaction triggered outcomes from the blockchain. https://ethereum.stackexchange.com/questions/383/what-is-a-dapp

[2] https://hbr.org/2017/03/global-supply-chains-are-about-to-get-better-thanks-to-blockchain March 2017, Harvard Business Review published an article entitled "Global supply chains are about to get better thanks to blockchain". http://uk.pcmag.com/amazon-web-services/87703/feature/blockchain-the-invisible-technology-thats-changing-the-world August 2017, Rob Marvin of PC Magazine published his take on the advances enabled by blockchain technology.

[3] https://medium.com/@peteratomic/intro-to-crypto-economics-9508e471d617 Peter Harris published a recommender list of crypto-economy and crypto-ecosystem reading in July 2017.

1.3 Research Objectives

The challenge in this research is to identify an optimal research process from which to develop software artefacts that utilise blockchain-enabled technology in such a way as to maximise the potential of the technology and enhance the real-world business application. The research comprises a literature review, a proof-of-concept scoping process and the development of a prototype software artefact. The scoping process will explore peer-to-peer and decentralised technologies and their potential to enhance process management at a high-profile organisation currently undergoing redevelopment: Bohemian Football Club (BFC)[4].

1.4 Research Methodologies

State-of-the-art business development models: Business Process Management (Mendling et al, 2017) and the Capability Maturity Model (Wang et al, 2016) are introduced. A set of Blockchain Feasibility Guidelines (Wang et al, 2016) are introduced that identify a set of common attributes for blockchain-enabled applications. The purpose of introducing these methods is to elaborate a set of desirable system traits for a new system model.

In order to identify and test potential blockchain use-cases in the wild an open innovation strategy is adopted. A two-phase orchestration model is designed in order to reveal as many potential use-cases as possible for deployment in a real-world context: Bohemian FC.

The orchestration model offers a qualitative iterative, distributed modelling process informed by state-of-the-art frameworks, to scope appropriate blockchain-enabled process improvements at Bohemian FC.

[4] http://bohemianfc.com

1.5 Scope and Limitations

The scope is limited to discovering and implementing blockchain-enabled use cases in the context of Bohemian FC. Any use case that utilises blockchain technology will be considered. Cryptocurrency valuation and trading are out of scope in this proof-of-concept research.

1.6 Document Outline

The literature review begins with an overview of distributed autonomous organisation (DAO). The blockchain is identified as an example of DAO. Blockchain technology is explored from multiple perspective including: vulnerability, resilience and maturity and a number of analyses are conducted.

Three state-of-the-art innovation frameworks are described: Distributed Digital Innovation, Business Process Management and Capability Maturity Modelling, with a view to discovering useful approaches to inform a research strategy. Lastly the context under review, Bohemian Football Club is described.

In Chapter 3, the design of an original two-phase orchestration model is defined. The model includes both a discovery and implementation phase. The key driving technique is a multi-level design and the documentation framework follows the success model of business process redesign identified by Vanwersch et al, (2016).

The implementation of the two-phase orchestration model is described in Chapter 4 and the process is documented according to six key procedural elements identified in the BPR success framework.

In Chapter 5, an evaluation of the orchestration model reveals the strengths and weaknesses of the strategy. The orchestration model and multi-level design technique are deemed successful if the process leads to the identification of at least one implementable blockchain-enabled system at Bohemian FC. Areas for future study are also identified.

All references and citations are contained in the Bibliography.

The Appendices contain supplemental content that may assist the reader in understanding the scope of work undertaken:

Appendix A – Summary of fieldwork

Appendix B – Code excerpts from proof-of-origin prototype

Appendix C – Multichain set up and CLI command notes

2. LITERATURE REVIEW

2.0 Introduction

This literature review begins with an overview of distributed autonomous organisation (DAO). What constitutes DAO is examined and the most successful instance, the Internet, is referenced (Berners-Lee, 1989). By considering the Internet in this context the benefits of distribution over centralisation as an organising principle, are reviewed.

The blockchain is also an example of DAO. It can be defined as a secure, consensus-based, decentralised public ledger that stores information immutably, on a peer-to-peer network. Core concepts associated with the blockchain derive from multiple sources. While the ongoing relevance of some or all of these concepts for the future of digital cooperation remains to be seen, select sources from diverse disciplines are introduced: law (Szabo, 1997), cryptography (Nakamoto, 2009; Woods, 2014; Buchman, 2015) and game theory (Schelling, 1960; Buterin, 2017). Each of these three influential fields, reflect the qualitative aspects of external research into new digital channels and associated user behaviours (Nylén & Holmström, 2015), that are part of the outward-looking, digital innovation process.

Details about consensus models are considered and a comparison between blockchain implementations, Hashgraph and a well-established key-value database, Google Bigtable is offered. The implications of this comparison will feed directly to the development of a proof-of-concept process and artefact arising from the purposeful scoping of the domain to determine appropriate business applications for blockchain enabled technologies.

Contemporary thinking on business process innovation is introduced with an overview of Distributed Digital Innovation (Nylén & Holmström's, 2015; Von Hippel & von Krogh, 2016; Nambisan et al, 2017). Defining what it is, exploring its conceptual origins and selecting key elements relevant to the work in hand. Adopting digital innovation methods requires an interrogation of the assumption that exploring the potential of peer-to-peer and decentralised technologies in this context, is a valid approach.

State-of-the-art business development models: Business Process Management (Mendling et al, 2017), the Capability Maturity Model (Wang et al, 2016) are introduced. A set of Blockchain Feasibility Guidelines (Wang et al, 2016) are introduced that identify a set of common attributes for blockchain-enabled applications. The purpose of introducing these methods is to elaborate a set of desirable system traits for a new system model.

Lastly, a brief description of the context for the research, Bohemian Football Club is given. Bohemian FC is a professional football club and its senior team participates in the Football Association of Ireland's Airtricity League. It is a membership organisation with a highly distributed governance model, managed by a voluntary Executive Board.

2.1 Decentralised Autonomous Organisation

A decentralised autonomous organisation (DAO), not to be confused with 'The DAO'[5], is a structured, distributed group agreeing to participate in collective endeavour but not to be facilitated by centralised decision-making (Buterin, 2014). The internet is perhaps the best known and front-runner in a global distributed information-sharing system. Tim Berners-Lee first proposed an early version of the internet called 'Mesh' in 1989. He hoped that management at the CERN Research Centre would adopt 'Mesh' as a distributed hypermedia system that facilitated "information sharing about complex, evolving systems" and was built on top of another 'complex and evolving system'[6], the global peer-to-peer network we are now widely familiar with, the internet.

[5] The DAO, an ill-fated firm launched on the Ethereum blockchain which was robbed of up to 30% of its value (approx. $70 million) in an anonymous criminal act known widely as the DAO Hack.This forced a controversial 'hard fork' (June 2017) in the Ethereum blockchain, splitting what continues to be known as Ethereum (ETH), from the original, which is now called Ethereum Classic (ETC). Users who took a stand against the hard fork didn't upgrade their software and continue to mine on the classic blockchain which was forked at block 192000.

[6] Text of Tim Berniers Lee's proposal available at W3 Archive. https://www.w3.org/History/1989/proposal.html

While the human-scale, decentralised, user requirements to create the internet were well-specified from the outset, the distributed, peer-to-peer network it is built on was not (Berners-Lee, 1989; World Wide Web Consortium[7], 1990).

Today, the internet shares a phenomenal amount of information. Core messages (e.g. web-pages) are navigated and discovered via the client-server distributed architecture model to serve web-page content to browsers. Network meta-messages (e.g. origin and destination headers) and hardware gossip[8] are transmitted across a massive peer-to-peer hardware network. (Cisco, 2017).

There are in essence two approaches to computer systems architecture: centralised and distributed, seen here in Figure 2.1. Decentralisation is a hybrid of both, whereby numerous centralised hubs are interconnected.

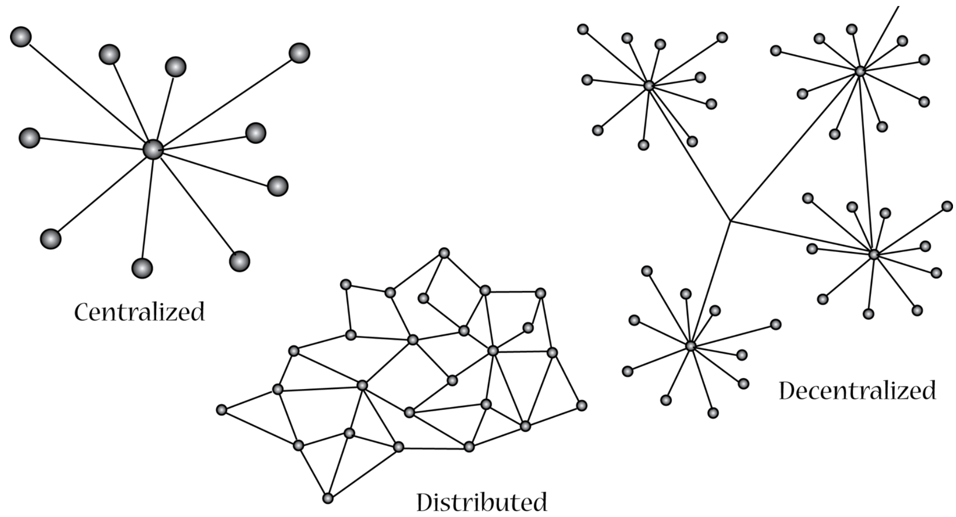

Figure 2.1 Models of system architectures: distributed, decentralised, centralised. Source: (Baran, 1964)

The decentralised architecture has many proponents and applications, an example being the popular and robust client-server architecture of web-applications where the workload of a web-service is partitioned between the request-making clients and the response generating servers.

[7] W3C - Oct 1990, new proposal for finding to develop world wide web at CERN. https://www.w3.org/Proposal.html
[8] Peer nodes broadcast their 'up' status every 2-5 seconds, facilitating rerouting when necessary.

A fully distributed or peer-to-peer architecture also has many advocates and applications: internet-of-things, electricity supply networks and telecommunication networks are examples. Blockchain is merely one of the latest utilising a distributed organising principle.

The internet developed in a way that facilitated maximal access, with minimal barriers to entry, for the purpose of sharing information between humans. It offered more-or-less open access[9] to a purposefully decentralised system, operating under distributed governance, according to a set of pre-agreed rules of participation (Berners-Lee, 1989). Within ten years it had spawned a world-wide 'information super-highway'[10] the bedrock of e-commerce and mobile business channels.

The nascent permanent web or Interplanetary File-System (IPFS), (Benet, 2014). IPFS offers a distributed solution to permanent, online resource location, using peer-to-peer networking rather than centralised server systems to host online resources. In essence, this means that in the current iteration of the internet, a unique resource locator (url) points to a location of a web document on a server (w3.org, 2017). In IPFS the url points to the item itself, wherever a copy of it is held, utilising peer-to-peer swarm technology to link nodes. IPFS' creators seek to shift the concept of the internet away from the client-server model on which internet 2.0 is based, towards a fully distributed model (Benet, 2014).

This approach to a potential future for internet services, underpins how a distributed architecture offers something different to the ecosystem: a permanent, versioned archive of web content. It expands the purpose of the Web Archive's Wayback Machine[11] project that arose from a recognised need to capture for posterity, research and archival purposes snapshots of the internet for future reference.

In his seminal work, Formalising and securing relationships on public networks, (1997) Nick Szabo describes how new "protocols running on public networks, both challenge and enable us to formalize new kinds of relationships in the new

[9] Open access - in 1989, few people outside of research (either academic, military, industry) had access to networked computers. There was a greater assumption of trust in users than there is on the world wide web today.
[10] Information super-highway - a term variously attributed to both Korean-American 1st generation video artist Nam June Paik and US politician and environmental activist Al Gore.

environment". The environment referred to is the nascent internet-enabled social order of the late 1990's. Szabo describes this environment as a liberation for economic and social development and hones in on the context of contract law and property ownership in particular. He imagines how, in the future, entities he calls 'smart contracts' will simplify and streamline the long-standing legal, transactional model we humans have developed over thousands of years (Szabo, 1997; 1998).

Almost thirty years later, DAO technology and platforms have the potential to facilitate a new wave of digital innovations which leverage the potential of an immutable, distributed, public record of transactions to reshape trade relations and consumer trust (Szabo, 1997; Nakamoto, 2009; Buterin, 2017; Buchman, 2016; Epicentre, 2017).

2.2 Vulnerability, Resilience and Maturity.

2.2.1 Vulnerability

From the early days of the internet to date, our expectation of good-behaviour on the internet has diminished. Online financial services, social media and e-commerce involve the use of digital identities and in the past eight years, 7.1 billion online identities have been exposed as a result of data breaches (Symantec, 2017) and the Internet has become a target for online criminals (Khan, 2016). Symantec, a commercial online security corporation, continues to release annual Internet Security Threat Reports (ISTR).

Perhaps not surprisingly, there have also been a number of significant assaults on blockchain systems, including the aforementioned 'DAO Hack' (2015) and more recent Parity Hack[12] (Nov 2017). Both occurred on the Ethereum platform.

[11] Wayback Machine - a digital library of Internet sites and other cultural artefacts in digital format. web.archive.org
[12] Parity Hack - On 6 Nov 2017, devops199, a self-coined 'eth-newbie', accidentally set himself as the owner of a library contract and then killed the contract. devopps199 has since removed all trace from internet forums(user: ghost here,https://github.com/paritytech/parity/issues/6995 explains how he did it). The template was the source contract of multiple ICO wallets and the accident caused the loss of all funds contained in the wallets associated with those contracts.

While the DAO Hack was purposeful and malicious, leading to the theft of over $70million, it appears the Parity Hack was accidental and due to poor programming practices, causing the loss (not theft) of over $150 million. Both are examples of zero-day vulnerabilities in blockchain applications. As seen in Table 2.1, zero-day vulnerabilities are common enough and continue to be discovered and exploited, they offer potentially lucrative opportunities to cybercriminals.

Symantec Internet Security Threat Reports, 2016 - 2017			
	2014	**2015**	**2016**
Vulnerabilities			
Zero-day weaknesses discovered (unknown to owners)	4,958	4,066	3,980
Total no. breaches reported (est. 85% unreported)	1,523	1,211	1,209
New malware variants	275mill	355mill	357mill
Computers participating in botnets*		91.9mill	98.6mill
Ransomware: Number of detections		340,665	463,841
Ransomware: Average ransom amount	$373	$294	$1,077
Average losses caused by ransomware	-	$100mill	$500mill

Table 2.1 Vulnerability overview 2016 and 2017 Symantec ISTR datasets.

The extent of user vulnerability to identity theft or perhaps less-detrimentally, exposure to ‘trolling’ behaviour online (abusive personal attacks on public forums, often made by anonymous users targeting individuals or whole communities) are just two ways that online behaviour exhibits less than trustworthy traits. Yet, in any cooperative system, there is a need for participants to act in good faith. In a cooperative system, where participants can be anonymous or can act without consequence, that need is greater.

It is, in some sense, possible to view the public blockchain ecosystem as a sort of commons. As such, it is vulnerable to the threats identified as pollution in Hardin’s 1976 paper The Tragedy of the Commons, where actors pollute the public blockchain ecosystem simply because it’s there and they can. This pollution can exist as malfeasance and untrustworthy behaviour, a sort of corruption of the messaging processes associated with the blockchain.

For Hardin, there is no successful way to curb the impetus to pollute the commons. He identifies inadequate solutions as community-imposed taxes and regulations. In blockchain these can be recognised as incentives and disincentives for / against, good behaviour / malfeasance. For example, in Proof-of-Stake consensus, validators (the proof-of-stake version of a miner) are required to provide substantial sums of native token as collateral against rogue behaviour (Buchman, 2015).

In many types of distributed systems good behaviour is incentivised and malfeasance dis-incentivised. This is also true of blockchain systems. In game theory, deterministic behaviour models make an assumption that actors will at the very least behave rationally, in a way that is beneficial to their own welfare (Schelling, 1960). However, it has not been found that humans behave rationally in a formal analysis of smart contract participants using game theory (Bigi et al., 2015; Norta, 2016).

Hardin (1976) claims that “the social arrangements that produce responsibility are arrangements that create coercion [and] an infringement on freedom.” He calls this duality a double-bind situation and is counterproductive. Hardin advocates for the end of the commons. In the blockchain ecosystem, an end of the commons may be mirrored in a move towards private blockchain adoption (Coindesk, 2017).

Li et al (2017) have conducted a thorough survey of the security of blockchain systems, summarised in Table 2.2.

They note the two distinct phases of blockchain development: Blockchain 1.0 when the technology was used largely for cryptocurrencies (Bitcoin, Litecoin, Dogecoin amongst 700+ cryptocurrencies) and Blockchain 2.0 with the advent of Turing complete languages for smart contract development.

Risk	Cause	Range of influence
51% vulnerability	Consensus mechanism	Blockchain 1.0, 2.0
Private key security	Public-key encryption scheme	
Criminal activity	Cryptocurrency application	
Double spending	Transaction verification mechanism	
Transaction privacy leakage	Transaction design flaw	
Criminal smart contracts	Smart contract application	Blockchain 2.0: smart contracts
Vulnerabilities in smart contract	Program design flaw	
Under-optimized smart contract	Program writing flaw	
Under-priced operations	EVM design flaw	

Table 2.2 Taxonomy of blockchain vulnerabilities: adapted from Li et al (2017)

The four advantage fields of cryptocurrency include: Irreversible and traceable transactions, decentralised and anonymous activity, secure and permissionless participation (facilitated by cryptography and consensus mechanisms), fast and global transactions regardless of the geographical location of system users. Three of these offer significant advantages over traditional fiat currency transactions: anonymity, permissionless participation and speedy global transfer. It is clear to see why a large criminal enterprise such as Silk Road would accept payment in Bitcoin.

Further, Li et al (2017) describe Blockchain 2.0 as the introduction of smart contract execution on the blockchain. A smart contract is defined as a lightweight DApp (decentralised application) that can be executed on Ethereum or other blockchain (e.g. Stellar, Monax or Lisk).

The benefits of DApps are described as: automatic and autonomous code execution, stable and traceable activity (state replicated across every node), and secure (facilitated by cryptography and consensus mechanisms). Gideon Greenspan, CEO of Multichain publicly questions the requirements and real use cases for executing code on a blockchain over off-chain execution, given the issues for concurrency across a distributed network (Epicentre, 2017).

The Byzantine General’s Dilemma abstracts a theory of a Byzantine fault or malicious actor that succeeds in presenting different system views to different observers. Byzantine fault tolerance (BFT) defends against vulnerabilities that prevent components of a system from reaching consensus.) BFT fails at a 51% threshold, when a system becomes vulnerable to a 51% attack including Sybil spoofing attacks (forging identities in peer-to-peer networks in order to disrupt messaging and common-system view).

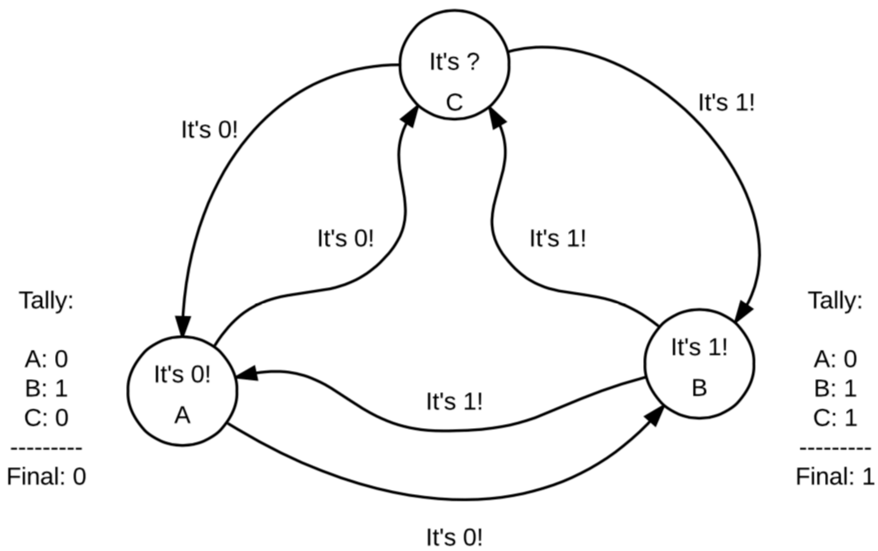

Figure 2.2 System obfuscation resulting from a single Byzantine fault. Source: Buchman, 2016.

As shown in Figure 2.2 a 51% vulnerability facilitates a number of attacks on a distributed system by manipulating and obscuring a common view of the system state: reverse transactions, double spending attack (the same coins are spent multiple times), exclude or modify transactions on blocks - this has additional significance in smart contract execution, interfere with honest mining, disrupt the confirmation of transactions and block ordering. (Li et al, 2017; Buchman, 2016; Buterin, 2014).

The additional vulnerabilities in blockchain 2.0 smart contracts arise from unforeseen consequences in contract execution. As contracts once initiated should operate autonomously the notion that 'code is law' and must at all costs maintain chain immutability has arisen. Others question this stance as simplistic and incomplete without a statement of what a smart contract can achieve (Coindesk, 2016). It has proven to be an inappropriate ethos given widespread poor development practices (multiple Parity hacks, The DAO debacle and multiple losses by individual developers reported on Reddit and other Fora), uncertain legal context and widespread association with criminal activity.

2.2.2 Resilience

Montelongo Arana & Wittek, (2016) write about community resilience and the challenge of motivating long-term cooperation in communities. This is relevant to the wider context of the community surrounding blockchain and cryptography in general.

In the current phase of its development, Ethereum in particular, facilitates a view of their users as a pioneering crypto-community. There is a wider sense that anyone active in the blockchain space, holding currency, writing smart contracts, building applications on blockchain are all part of the "crypto space".

Cryptography is a fundamental feature that underpins blockchain technology. Cryptography serves two functions in a blockchain. The first is to obscure private data in a public forum: the distributed public data-store or ledger. The second is to validate block order and achieve consensus among nodes (Nakamoto, 2009; Buterin, 2014; CeADAR, 2016; Woods, 2014; Kwon, 2014).

Closely allied with cryptographic consensus is the role of game theory to probabilistically determine group behaviour and incentivise honest action in a trust-less and often anonymous environment (Schelling, 1960).

Consensus is the agreement of block order. The role of assigning block-order is a powerful one and a potential single point of failure in a system. There are many strictures and guidelines in place to ensure, as much as is possible, that this aspect is safeguarded. In a distributed blockchain system this role is assigned to actors called 'miners' in a proof-of-work consensus model and 'validators' in a proof-of-stake consensus model.

There are numerous variations of proof-of-stake consensus. Swirld's Hashgraph website claim five approaches to achieving consensus on a distributed network: (1) Proof-of-Work (PoW), onerous computation (e.g. finding the next number in a sequence that ends in four zeros) to dissuade miners from identity spoofing and launching a Sybil attack. PoW is responsible for blockchain's reputation for squandering energy resources (O'Dwyer, 2014). (2) leader-based systems e.g. BFT, Paxos or Raft, (3) Proof-of-Stake (PoS), where native tokens are staked for validation role, when delegated it is known as DPoS (4) Vote, while possible in some distributed networks, is not considered appropriate for real time blockchain systems in the wild, (5) virtual vote, e.g. Hashgraph proxy vote, efficient because it doesn't require an actual vote.

In public systems, participants must prove either that they have executed a significant piece of processing in a proof-of-work consensus; or that validators have staked enough resources as collateral to deter against malfeasance in the proof-of-stake consensus model (Buterin, 2014; CeADAR, 2016; Woods, 2014; Kwon, 2014). The Bitcoin[13] blockchain utilises proof-of-work to achieve consensus.

An example of leader-based consensus is practical Byzantine Fault Tolerant (BFT) consensus solution based on Schelling's (1960) Byzantine General's Problem (Buterin, 2015). In BFT consensus all validators are randomly assigned the right to propose blocks. Agreement on which blocks are to be adopted occurs during a multi-round voting process, at the end of which, validators agree on which blocks form the chain. According to Schelling's theory, BFT consensus can continue to operate successfully with up to 1/3 of malicious actors in the validation pool. Tendermint's consensus protocol relies on BFT proof-of-stake consensus, as will Ethereum's forthcoming Casper release sometime in 2018.

[13] Bitcoin - currently the largest, most successful blockchain-enabled cryptocurrency. bitcoin.org

There are multiple blockchain implementations, they can vary in degree of trust attributed to the system: Multichain and Tendermint Core are suited to private, permissioned blockchains with a (relatively) high degree of trust (Buchman, 2015; Greenspan, 2014) and Ethereum Byzantium, a public blockchain implementation with disincentives for malfeasance in a low-trust environment (Buterin, 2015).

Consensus by vote can be achieved by polling all nodes as to their view of the correct state. This is achieved across networks and is subject to network latency and other delays.

Hashgraph, a newer alternative to blockchain, uses a different approach to consensus, using a proxy vote based on node-messaging meta-data called ‘gossip’. Hash graph continues to use the power of cryptography to secure privacy and relies on a version BZT to implement its protocol (Baird, 2016).

Blockchain 2.0, introduced the notion of smart contracts. While the concept of a smart contract may have its origins in the early days of the public internet, today the term ‘smart contract’, widely used in certain communities (crypto, blockchain), does not have the same meaning as that envisaged by Szabo in 1997. His vision of new network protocols spawning a new type of legally-binding agreement has yet to come about. Smart contracts today are scripts written in programming languages (e.g. Solidity, Serpent) in order to write and read data to and from the blockchain.

On the Ethereum network, Turing-complete languages are compiled and read to the Ethereum Virtual Machine (EVM). The Ethereum blockchain can trigger further actions, according to a set of pre-defined, pre-agreed rules e.g. A buyer receives an order of goods and payment triggers (Buchman, 2016; Wood, 2014; Wright & de Filipi, 2015).

Smart contracts have also facilitated the introduction of ‘oracle’ data into a smart contract. An ‘oracle’ is commonly understood to be off-chain data fed into a smart contract at a particular, predefined and expected point in its execution, in order to proceed to the next step e.g. a currency exchange rate at a given point in time, or a notice of delivery which triggers payment.

The issue of concurrency, locking and transaction ordering on Ethereum blocks becomes crucial as code can trigger outcomes that are unforeseen. It matters that each node has the same inputs to generate the same outputs when executing a smart contract (Woods, 2014; Buterin, 2014). Gideon Greenspan, CEO of Coin Sciences and Multichain questions how often it is necessary to a use case that a contract execute on a blockchain, as opposed to node or client-side (Epicentre, 2017).

To date, smart contracts have yet to be legally tested in any jurisdiction (Augustus Cullen Law in Irish Tech News, 2017) and blockchain transactions with their immutable, timestamped, public record have yet to be legally accepted as valid proof of any type of binding agreement (Epicentre, 2017).

2.2.3 Maturity

According to Herbsleb's Capability Maturity Model (1997), blockchain technologies are somewhere between the Initial and Repeatable Stages. It is clear there are many ad hoc aspects to a variety of implementations, the 'build fast and break things' mentality of developers still current. Many implementations of blockchain are neither stable nor reliable just yet.

Bitcoin's ongoing consternation about block size is stunting the networks growth. Outlets, including Steam, the online gaming service, Fiverr, the freelancer website have removed options to pay for goods using Bitcoin as the transaction costs are too high and validation takes too long. There is a go-slow on the implementation of Segregated Witness, following the cancelled SegWit2x fork[14] in mid-November 2017. The complicated tussle between core developers, the user community and Bitcoin miners over block size and the best way to grow the network grow is rife with conflicts

[14] SegWit2 fork: context found here: https://news.crunchbase.com/news/bitcoin-lost-way-means-exchange/

of interest, suspicions and accusations. However, it is outside of the scope of this research.

With blockchain, a roll-back is technically possible as exemplified by Ethereum's hard fork in June 2017. With a ransomware attack, a targeted user is largely powerless to roll-back their system to a point in time pre-hack. In this light rollback can be seen as a positive. However, the fundamental principle of blockchain is that it is immutable, unchanging, public and decentralised? So how can one actor e.g. 'blockchain administrator' take the decision to initiate a roll-back to save one set of users, when it will involve wiping out any other user transactions that have been recorded on the chain since?

There is a considerable amount[15] of internet chatter about the pros and cons of forking a blockchain to fix mistakes. Whether or not Ethereum will fork again in order to reverse the loss of upwards of 150million USD in Ether (the virtual currency in use on Ethereum platform) remains to be seen. It has been suggested that the fork could quietly occur in line with the next scheduled upgrade.

Suggestions such as these lead to concerns about governance, neutrality and sovereignty in distributed technologies. While technically, a system reversal is possible, debate[16] centres around who has the authority to decide when there is no means to affect a vote or mandate a decision?

Governance issues are a core aspect of maturity for the technology and affect the standing of implementations in Qualification and Selection of Open Source software (QSOS) evaluation model seen a little later.

As discussed earlier, Wang et al (2016), have concluded that blockchain technology is too immature to adequately assess using Capability Maturity Modelling. In an exploratory fashion, the Qualification and Selection of Open Source software (QSOS) evaluation model is partially adopted to examine more closely what state of maturity a

[15] www.reddit.com/r/ethereum/comments/4r2f73/when_is_the_dao_hard_fork_end_date/
[16] www.reddit.com/r/ethereum/comments/7f9xb4 parity_intends_to_offer_multiple_solutions_for/

set of blockchain implementations are at. The maturity criteria assessment[17] rates each of the blockchain implementations according to a simple 0-1-2 weighting scheme. The field headings include: legacy, activity, governance and professionalisation. Below the initial phase of the QSOS Maturity Criteria comparison is summarised, Table 2.3 details weighted criteria of the software under the Legacy heading: age, (trouble-shooting) history, core team and popularity or traction. As is evident, most implementations are no more than three years old at this point.

Blockchain Implementations		**A: Bitcoin B: Multichain**		**C: Ethereum D: Tendermint**		**E : Hashgraph**
• Legacy: project history and heritage		**A**	**B**	**C**	**D**	**E**
Age	0 : Less than 3 months 1 : Between 3 months and 3 years 2 : More than 3 years	2 (2009)	1 (2015)	2 (2014)	2 (2014)	1 (2017)
History	0 : The software has many problems 1 : No major crisis or history unknown 2: Positive crisis management history	0 (alt coins, block size, tx costs)	2	0 (hacks, forks, tx costs)	1 (Gaia testnet failure)	1 (patented not open source)
Core team	0 : Few core developers identified 1 : Few core developers active 2: Identified core development team	2	2	2	2	1
Popularity	0 : Few identified users 1 : Usage can be detected 2 : Many known users and references	2	2	2	1	0 (recent emergence from stealth mode)
	Totals	**6**	**7**	**6**	**6**	**3**

Table 2.3 Stage 1 QSOS evaluation: Legacy, history, heritage

Blockchain Implementations		**A**	**B**	**C**	**D**	**E**
• Governance and growth strategy						
Copyright owners	0 : Rights held by individual or commercial entity 1 : Rights held uniformly by many individuals 2 : Rights held by a trusted legal entity (eg: Apache)	1	1	1	1	0
Roadmap	0: No roadmap 1: Roadmap without planning 2: Versioned roadmap: planning and delay metrics	1	2	2	2	1
Project management	0 : No apparent project management 1 : Project managed by individual or single commercial entity 2 : Strong independence of the core team.	2	2	2	2	2
Distribution mode	0 : Dual distribution with a commercial version along with a functionally limited free one 1 : Subparts available under proprietary license (core, plugins) 2 : Completely open and free distribution	2	1	2	1	1
	Totals	**6**	**6**	**7**	**6**	**4**

Table 2.4 Stage 2: QSOS evaluation: Governance and growth strategy

Table 2.4 gives a breakdown of factors which indicate a mature and effective governance: ownership, roadmap, project management, and distribution mode.

[17] This set of maturity criteria is compulsory for every evaluation in the QSOS 2.0 format. It is distributed under the FDL2 license

The comparison is compiled in line with research into each product. Sources include individual product websites[18], Github[19], Reddit[20], Twitter[21] and other community fora and information gathered from respected online publications: Crunchbase[22], Medium[23], Hackernoon[24] and Ars Technica[25].

Table 2.5 summarises overall results from the four criteria headings: legacy, activity, governance and professionalisation.

Blockchain Implementations	Bitcoin	Multichain	Ethereum	Tendermint	Hashgraph
• Legacy: Project's history and heritage	6	7	6	6	3
• Activity	4	7	4	5	2
• Governance: Project's strategy	6	6	7	6	4
• Professionalisation / industrialisation	6	7	4	4	4
Totals	**22**	**27**	**21**	**21**	**13**

Table 2.5 QSOS evaluation Summary Review

Multichain comes out on top, followed by Bitcoin, then Ethereum, Tendermint and Hashgraph. The QSOS Maturity Criteria proved influential in the blockchain selection made in the later stages of the proof-of-concept process.

In tandem with a technology's maturity, it is important to consider the wider context into which it is being launched. Blockchain's role as a vector of disruption, is largely associated with its potential to facilitate disintermediation: getting rid of the middle-man to oversee, authenticate or give assurance to a process. Often these roles are filled by jurisprudential actors: notaries, solicitors, or agents. One popular blockchain use case is the online notarisation proposition known widely as 'proof-of-existence', used

[18] Websites: bitcoin.org, multichain.com, ethereum.org, tendermint.com, hashgraph.com
[19] Github a web-based version control repository hosting service, mostly used for computer code. It facilitates collaboration github.com
[20] Reddit an Advance Publications (also own Conde Naste) a social news aggregation, content rating, and discussion website. Registered members submit content to themed sub-reddits which are then voted up or down by other members. reddit.com
[21] Twitter a popular social channel for asynchronous, public commentary and debate. twitter.com
[22] Crunchbase "was founded to be the master record of data on the world's most innovative companies." news.crunchbase.com/sections/crypto/
[23] Medium "brings you the smartest takes on topics that matter. It offers a space to further the conversation not sell it." medium.com/topic/technology
[24] Hackernoon is a Medium publication and part of the AMI publication group that own & operate community driven publications. It claims to be "How hackers should start their afternoons." hackernoon.com/

to record IP authorship e.g. original image or sound files or access to / ownership of a file at a given point in time.

The legal context evokes high-level social constructs, such as ‘transaction’ and ‘ownership’ (Szabo, 1997; 1998). The new term ‘crypto-law’ which the Electronic Frontier Foundation[26] uses, refers to the use of legal means to protect cryptography as a source of privacy on the web, and not as Szabo (1997) may have done, to reformat the role of the legal contract in response to the affordances of digital networked economies.

A legal team at Augustus Cullen Law, in response to questions from online publication Irish Tech News[27], describe the situation in Oct 2017:

> “The blockchain technology is currently not subjected to any specific regulations and laws. Subsistence laws are customarily applied to new technologies as they emerge, and it is uncommon that a new law is introduced immediately in reaction to the emergence of new technology. Lawmakers across Europe are looking to understand more about blockchain technology before implementing rules. This ‘wait-and-see’ approach avoid[s] applying rules prematurely that might potentially prevent blockchain industry growth.” Augustus Cullen Law as reported by Mitsu Fonseca of Irish Tech News (2017).

It is my opinion that the potential for widespread adoption depends upon a legal recognition of the public role of blockchain. Blockchain may be recognised as having valuable notarisation potential leveraging the public, time-series record of transactions. As an executer of smart contracts that have standing in the real world and not only as virtual commodities for virtual communities online, the blockchain may come to maturity as a facilitator of legal conveyancing. Research into technology acceptance models and how they might relate to blockchain (in BPM and business generally) are identified as important future work (Mendling, 2017; Venkatesh, 2014).

---

[25] Ars Technica is Conde Nast's only digitally native editorial publication “a trusted source for technology news, tech policy analysis, breakdowns of the latest scientific advancements.” arstechnica.com/

[26] Electronic Frontier Foundation - not-for-profit organisation seeking to protect freedom of speech, access and participation on the internet. https://www.eff.org/about

2.3 Distributed Datastores: Blockchain, Hashgraph & Bigtable

2.3.1 Blockchain

Blockchain, (Buterin, 2014; Buchman, 2015;) is essentially a chain-like data structure, comprised of blocks, which in turn, are comprised of bundles of data, added to a block as an individual transaction. A distributed blockchain, requires a consensus algorithm to facilitate common block-ordering across multiple nodes. Table 2.6offers a summary of blockchain platforms available at the end of 2017.

Platform	Start Date	Domain	Best features
Bitcoin	2009	Cryptocurrency	Longevity, user-base, currency value.
Corda	2015	Finance	Secure, strictly-private, highly scalable.
Ethereum	2014	Smart contract execution	Turing complete EVM, public blockchain.
Hyperledger	2015	Distributed asset ledger	Umbrella project for open source blockchain projects from Linux Foundation.
Multichain	2014	Distributed asset ledger	Bitcoin compatible, permissioned smart ledger, flexible design, implementation and scaling.
Tendermint	2014	Distributed asset ledger	Private, permissioned, flexible, scalable.

Table 2.6 summary of blockchain platforms available at the end of 2017

Three Open Source blockchain implementations are given further consideration in Table 2.7. These include: Ethereum, Multichain and Tendermint.

Feature	Ethereum (2014)	Multichain (2014)	Tendermint (2016)
Installation dependencies	Geth, EVM, Mist or other wallet: pay by Gas.	Multichain (+ wallet if using currency transactions (tx))	Go, Tendermint (+ wallet if using currency tx)
Synchronising	Public - days	Permissioned - n/a	Permissioned - n/a
Set-up	multiple dependencies and versions to synch.	CLI installation onto node server or docker image	CLI installation
Interfaces	JSON-RPC API, Geth-CLI, Geth-Explorer.	JSON-RPC API, Multichain-CLI, Multichain-Explorer.	JSON-RPC API, ABCI-CLI,
Written in	C++, Golang, Rust	C++	Golang
Compatible with	Solidity, Serpent, LLL, Mutan, Viper.	Modern programming langs via json-rpc API.	Any language via ABCI interface.
Tutorials	yes	yes	yes
Versions	4	29	unknown
License	GPLv3, LGPLv3	GPLv3	Apache License 2.0

Table 2.7 Comparative analysis of three Open Source blockchain implementations.

[27] Irish Tech News - article by Mitsu Fonseca, 16/10/17 irishtechnews.ie/the-impact-of-blockchain-on-legal-environment/

2.3.2 Hashgraph

A hash graph utilises a different data structure to the blockchain. It is a mesh-like graph-stack that is ordered by agreement through consensus achieved by analysing metadata associated with message-sending between nodes. This process is called 'gossiping about gossip'[28] and underpins the consensus model of newcomer Hashgraph (Baird, 2016). Table 2.8 facilitates a comparison of Hashgraph with blockchain implementations in Table 2.7.

Feature	Hashgraph (2017)
Installation dependencies	SDK, Java
Synchronising	Permissioned - n/a
Set-up	-
Interfaces	JSON-RPC API, Geth-CLI, Geth-Explorer.
Written in	C++, Golang, Rust
Compatible with	Solidity, Serpent, LLL, Mutan, Viper.
Tutorials	yes
Versions	4
License	Patent

Table 2.8 Analysis of Hashgraph for comparison with blockchain implementations in

IOTA Foundation offers a similar mesh-like data structure called Tangle facilitating the Internet of Things domain. It is out of scope for this research as it is so new: Serguei Popov's whitepaper was published in October 2017.

2.3.3 Google Bigtable

Bigtable is a sparse, distributed, persistent, multi-dimensional, time-stamped, sorted map. Its architecture can span multiple servers or nodes, in a highly available, fault tolerant implementation. Bigtable does not support a relational data model; instead the value is an object which is highly structured into columns. Columns are grouped together in sets called column families the system allows columns to be sorted lexicographically and timestamped. (Ghemawat, 2003; Chang, 2016). It can be conceptualised as a distributed key / value data store for large amounts of structured data. A more flexible and scalable data solution than either blockchain or hash graph.

In terms of data solutions, we can model and implement scenarios where different databases are used collaboratively. Cloud Bigtable has something to offer, in this wider view. Table 2.9 details a features comparison between Google Bigtable, Blockchain and Hashgraph:

Features || Model	**Bigtable (2004)**	**Blockchain (2009 - to date)**	**Hashgraph (2017)**
Relational nature	No	No	No
Developer	Google Inc	various	Swirlds Inc
Written in	C++	Golang (mostly)	Java
Query language	APIs in C++	APIs - JSON-RPC	API in Java
SQL nature	CLI	CLI	CLI
High availability	Yes	Yes	Yes
High scalability	Yes	Yes	Yes
Single point of failure	No	No	No
Open source	No	Some implementations are	No
Versioning	Yes (built-in timestamp)	Immutable	Immutable
Indexing	On map, timestamped	On chain, timestamped	On hashgraph, timestamped
Data Processing	Batch processing, Single atomic transactions.	Smart contracts, Multichain raw transactions, Single atomic transactions.	Smart contracts, Single atomic transactions.

Table 2.9 Features comparison between Google Bigtable, Blockchain and Hashgraph

2.4 Distributed Digital Innovation

Distributed Digital Innovation (DDI), a framework proposed by Nylén & Holmström, (2015) describes how digital evolution is forged from a series of interconnected and loosely defined elements. A key aspect includes 'environmental scanning', a speculative, outward-looking process, that involves external research including new digital devices, channels and associated user behaviours.

[28] Gossiping about gossip - leverages knowledge afforded by the meta-data passed across the network in a process known as gossip in order to determine at any given point how a node 'would have voted' to achieve an ordering consensus (Baird, 2016).

Nylén & Holmström's (2015) approach originates in Chesborough's (2006) well-regarded concept of 'open innovation'. Open innovation is a process of 'outside-in' analysis of "purposive inflows and outflows of knowledge" (Chesborough, 2006) accelerating both internal innovation and expanding markets for external use of the products of open innovation. In this instance, it is possible to frame this proof-of-concept process and resultant artefact as an internal innovation arising from a specific context which has the potential to expand to other related business use-cases.

Akin to Nylén & Holmström's (2015) distributed digital innovation framework, Von Hippel and von Krogh (2016) also place a focus on analysing contexts, both external and internal, during product innovation. They describe "dynamic problem–solution design pairing" as a temporary matching or an instance of needs, user behaviours, digital artefact features and other "sociotechnical constellations" or zeitgeist.

In each of these instances, time and openness to innovation, are identified as key components to the successful derivation of new products, processes or services. (Nylén & Holmström's, 2015; Von Hippel and von Krogh, 2016; Nambisan et al, 2017). A thorough examination of the potential solutions offered by distributed technologies may then be paired up with priority areas identified during the analysis phase of the system under review.

Namibisan et al (2017) challenge traditional assumptions about the bounded and centralised approaches required for innovation management. They recognise innovation agency as neither centralised nor predictable. Importantly, innovation outcomes are not seen as arising independently of process management. In addition, Namibian et al (2017) describe the usefully fluid boundaries inherent to digital innovation, as exemplified by environmental scanning and dynamic problem–solution design pairing.

These fluid boundaries are an important feature of the distributed digital innovation process where, of necessity, there are vested interests in researching, anticipating and negotiating shared and competing needs of collaborating partners. Time and an openness to innovation are important requisites to the success of a distributed digital innovation process. Valuing these traits is key to the development process and facilitate an agile approach to the development lifecycle.

For the purpose of this proof-of-concept paper, it is anticipated that both environmental scanning (Nylén & Holmström, 2015) and dynamic problem–solution design pairing (Von Hippel and von Krogh, 2016) will highlight potential candidate processes for innovation. With an additional emphasis on a distributed model of innovation, it remains to be seen what additional benefits to the process of digital innovation arise.

2.5 Business Process Management (BPM)

BPM is a state-of-the-art business management framework used to guide evolutionary process management. It encompasses design, implementation, evaluation and improvement of business processes. In mid-2017, a team from the German research body, Hasso-Plattner-Institute submitted a paper to ACM Transactions on Management Information Systems that explores the potential blockchain technology can offer to business process management (Mendling et al, 2017).

While recognising the success of BPM in streamlining intra-organisational processes, Mendling et al, (2017) note that challenges for streamlining inter-organisational processes include the difficulty of executing joint design process and a lack of trust. The team give consideration to the impact of blockchain across six core BPM capability areas as described by Rosemann & vom Brocke (2015): strategic alignment, governance, methods, information technology, people, and culture.

In terms of strategic alignment (Mendling et al, 2017) it is important for organisations to develop strategic priorities for any blockchain-enabled process and to identify clear risks that exist too. As a disruptive, disintermediation process-enabler, blockchain represents a threat to an existing status quo as much as it heralds fresh opportunities (Epicentre, 2017; Guo & Liang, 2016).

The governance models associated with BPM refer to appropriate, accountable and recognised roles and responsibilities for BPM projects (Rosemann & vom Brocke, 2015). Inbuilt BPM processes acknowledge challenges in relation to actor agency and incentivising participant behaviour (governance, people and culture are three of the six core capabilities in BPM introduced here). In an outward looking model, Blockchain may alleviate these issues in a co-operative inter-organisational context; or it may import an entirely new set of conflicts and challenges.

The failure of 'The DAO', the hard fork and subsequent splitting of the Ethereum chain into Ethereum Classic (ETC) and Ethereum (ETH) is a clear example of the unforeseen consequences of process management with ill-defined roles, agency and unexpected motivations.

The third core capability of BPM, encompasses the exploitative methods used, in the first place to uncover the weaknesses of existing processes, alongside methods to innovate existing processes or new processes entirely. Mendling et al (2017) make a comparison between the opportunities created by the emergence of distributed blockchain architecture to those of the early 1990's when the emergence of the client-server architecture allowed for widespread process re-engineering:

"In the early 1990s, Hammer & Champy [1993] formulated their credo of "Do not automate, obliterate:" companies should re-engineer their processes from scratch by the help of then new client-server technology instead of automating old-fashioned and ineffective ways of operation. Now, it is blockchain that provides the potential to re-engineer processes from scratch." Mendling et al (2017) p9.

The fourth BPM capability is Information Technology (IT) and includes all IT systems that support a business process. Blockchain-enabled systems will require new integrated development environments, new software models and sometimes new programming languages. They'll also require new threat-models for security and privacy. Limitations of blockchains must also be understood: data storage capacity, network utility (throughput, latency and bandwidth) and processing and computation power are drawbacks to use of public blockchains. Mendling et al (2017) and Gideon Greenspan on Epicentre (2017) suggest a possible adoption of only the desired design elements of blockchain, a time-series transaction history, for example, or the use of private chains for efficiency and simplicity.

The fifth and sixth capabilities are: people and culture. It is clear that any given BPM process will require new expertise across IT, business analytics and requirements engineering fields. In relation to blockchain-enabled processes in particular, additional skills in collaboration, partnership and contract management, software engineering and cryptography are desirable (Mendling et al, 2017).

Business Process Management - 6 Core Capabilities (Rosemann & vom Brocke, 2015)		
6 core capabilities of BPM and how they relate to blockchain adoption - a summary (Mending et al, 2017)		
1	Strategic alignment	As a disruptive, disintermediation process-enabler, blockchain represents a threat to an existing status quo as much as it heralds fresh opportunities. Risk assessment and strategic policies are desirable.
2	Governance	Inbuilt BPM processes acknowledge challenges in relation to actor agency and incentivising participant behaviour. In an outward looking model, Blockchain may alleviate these issues in a co-operative inter-organisational context; or it may import an entirely new set of conflicts and challenges.
3	Methods	Methods in BPM encompass the exploitative methods used to uncover the weaknesses of existing processes, alongside methods to innovate existing and new processes. Blockchain offers potential to re-engineer processes from scratch.
4	Information Technology	Blockchain-enabled systems will require new integrated development environments, new software models and sometimes new programming languages. They also require new threat-models for security and privacy. Limitations of blockchains must also be understood.
5	People	A BPM process will often require new expertise across IT, business analytics and requirements engineering fields. In blockchain-enabled processes, additional skills in collaboration, partnership and contract management, software engineering and cryptography are desirable.
6	Culture	It is suggested that blockchain is likely to lead to a more open and flexible organisational culture, further research into competing values models is suggested.

Table 2.10 Core capabilities of BPM and blockchain adoption - a summary (Mending et al, 2017)

From the cultural perspective, it is suggested that blockchain is likely to lead towards a more open and flexible organisational culture, this is a fairly speculative claim from Mendling (2017) who recommends further research into competing values models (Cameron & Quinn, 2005) to predict impact. Table 2.10 summarises the key points.

Mendling et al (2017), Greenspan on Epicentre (2017) and Augustus Cullen Law on Irish Tech News (2017) recommend devising blockchain-based collaborations within existing regulations, to ensure the process doesn't get bogged down in litigation. Key regulatory elements will influence both the context and success of blockchain-enabled process adoption: EU GDPR Compliance (Jan 2018), US SEC ruling that many ICO offerings are securities (July 2017), Chinese government shut-down of cryptocurrency exchanges (Nov 2017).

The BPM approach offers a fulsome, well-proven framework for exploring blockchain's potential to optimise or redesign existing processes. As previously stated, BPM traditionally handles governance from the intra-organisational perspective. Blockchain, it is anticipated, will allow for an outward-facing, co-operative approach that is consistent with a DDI approach.

2.6 Capability Maturity Model (CMM)

ACM Computing Classification System (ACM, 2012), a well-regarded classification system for Computing and Information Systems, recognises that in terms of technology, system and process maturity are measured across four fields: networks, information systems, computing methodologies and security / privacy. CMM is commonly used to guide the course of requirements gathering and subsequent phases of software development (Wang et al, 2016).

The framework can be used to make a determination about the maturity or appropriateness of adopting a particular process or module as a dependency in a project. In essence it makes a determination about stability and reliability. Capability maturity modelling may also be applied to organisational structure, management hierarchies, product supply systems or any other system comprised of interacting or 'moving' parts (Wang et al, 2016).

In this research, CMM is applied to distributed technologies and their potential, and to the information systems and organisation structure of Bohemian FC, the organisation under review.

To determine the maturity level of a product, process or service, assessment within a 5-stage maturity cycle is made (Herbsleb et al., 1997).

The stages of maturity are outlined in Table 2.11 below.

Capability Maturity Model (Herbsleb, 1997)		
5 stages of the maturity cycle		
1	Initial	ad hoc, potentially chaotic status of a new a product, process or service.
2	Repeatable	insights are garnered from similar products, processes or services.
3	Defined	when a product, process or service is standardised and documented.
4	Managed	standardised metrics for qualitative evaluation are in place.
5	Optimised	ongoing optimisation and improvement cycles are in train.

Table 2.11, 5 stages of the maturity cycle. Source: Herbsleb, 1997

2.6.1 Blockchain Feasibility Guidelines

Blockchain technologies are currently experiencing peak hype[29] and inflated expectations according to Gartner's hype-cycle for emerging technologies report (2017). The public attention on surging Bitcoin and other cryptocurrency valuations has attracted many to the blockchain ecosystem. It is not clear that a majority understand what the core capabilities of a blockchain system are.

Wang et al (2016), having concluded that blockchain technology is too young to be rightfully considered a mature system, propose a set of guidelines to assess the suitability of a blockchain solution for applications, summarised in Table 2.12.

Blockchain feasibility study (Wang et al, 2016)		
A blockchain solution has strong potential if at least four of the following apply		
1	Multiple parties share data	Multiple parties require views of common data
2	Multiple parties update data	Multiple participants take actions that need to be recorded and alter the data
3	Requirement for verification	Participants need to trust the validity of recorded transactions
4	Intermediaries add cost and complexity	Disintermediation has potential to reduce cost and complexity
5	Interactions are time-sensitive	Reducing delays has business benefits (e.g. enhanced liquidity, lower settlement risk)
6	Transaction interaction	Transactions created by different parties depend on each other

Table 2.12 Blockchain feasibility guidelines Source: Wang et al, 2016.

[29] Blockchain technology is reported to be close to the top of 'peak inflated expectations' according to Gartner's hype cycle for emerging technologies report 2017. http://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

Two additional phases are also identified: development and operations. The development phase includes: requirement analysis and architectural design. The operations phase recommendations include following a progressive replacement procedure where an existing system is being replaced.

This simple approach to determining the feasibility of a blockchain-enabled solution is a useful tool in scoping innovative and evolutionary process improvements for potential deployment of blockchain technology.

2.7 Bohemian Football Club

BFC is a professional football club and its senior team participates in the Football Association of Ireland's Eircom League. The Snr team is ranked 5th in the League 2017, the U19, U17 and U15 youth teams each won their League titles in 2017.

BFC home games are held in Dalymount Park, D7. The Club and Snr team are sponsored by Mr Green, an online gambling co. Bohemian Youth Academy is catered to by over 40 volunteer coaches with a youth membership of over 400 young players. Snr players may benefit from individual sponsorship and high-performing youth teams may also have team sponsors. Dalymount Park has three bars, an online and on-premises shop where merchandise is sold.

BFC Club is a voluntary organisation, governed by a voluntary board elected from within its membership. The Club establishes ad hoc committees to oversee key areas of its activities for example the Youth Committee. Its business concerns are managed across siloed strands within the organisation. It is an example of a distributed management structure with differing strands having distinct roles and budget-lines. It is clear from the outset that business processes can be streamlined with a more considered use of technology. Whether or not there is a role for blockchain technology in this process optimisation is discovered in the Methodology section later in this work.

2.8 Conclusion

This literature review began with an overview of distributed autonomous organisation (DAO). The blockchain is identified as an example of DAO. It can be defined as a secure, consensus-based, decentralised public ledger that stores information immutably, on a peer-to-peer network.

Blockchain technology is explored from multiple perspectives including: vulnerability, resilience and maturity and a comparison of three distinct approaches to distributed datastores was undertaken: blockchain, Hashgraph and Google Bigtable (as an example of a non-relational, time-stamped and distributed data store).

Three state-of-the-art innovation frameworks are described: Distributed Digital Innovation, Business Process Management and Capability Maturity Modelling, with a view to discovering useful approaches to inform a research strategy.

Lastly the context under review, Bohemian Football Club is described.

Chapter 3 describes the research design and methodology. It outlines a bespoke orchestration model, a multi-level design technique and a business process redesign success framework.

3. DESIGN AND METHODOLOGY

3.0 Introduction

In Chapter 3 the proof-of-concept research design and methodology are described. The research strategy follows an orchestration model of distributed digital innovation through two softly-bounded phases: discovery and implementation.

The pathway from discovery to implementation is documented according to a modified success framework which was adapted from a meta-model found in a systematic literature review of successful BPR approaches to system redesign (Vanwersch et al, 2016).

A four phase multi-level design technique is utilised to bridge the process from AS-IS system overview towards specification and implementation of proposed TO-BE blockchain-enabled systems.

The strategy is founded on a flexible, open innovation approach that relies on internal context-specific factors and external domain and environmental perspectives in order to discover process improvements.

Figure describes an overview of the orchestration model. The orchestration model allows for an adaptive process approach.

3.1 Orchestration Model

Distributed Digital Innovation (Nylén & Holmström, 2015) methods are well regarded for their openness, flexibility and unbounded edges. As identified in Chapter 2, Nambisan et al (2017) identify a number of approaches that prove useful for distributed innovation processes.

Orchestration is described by Nambisan et al (2017) as an opportunity arising from a sort of ‘floating around’ of problems awaiting solutions in a given context. This is noted to be particularly the case where an organisation is distributed and loosely structured. The orchestration they describe is one facilitated by digital technologies. In this research, a conceptual orchestration is deployed in order to discover potential use-cases for a specific type of distributed technology.

Environmental scanning is a key aspect of the distributed digital innovation framework (Nylén & Holmström, 2015). It describes how digital evolution is forged from a series of interconnected and loosely defined elements. Described as a speculative, outward-looking process, it involves external research including new digital devices, channels and associated user behaviours.

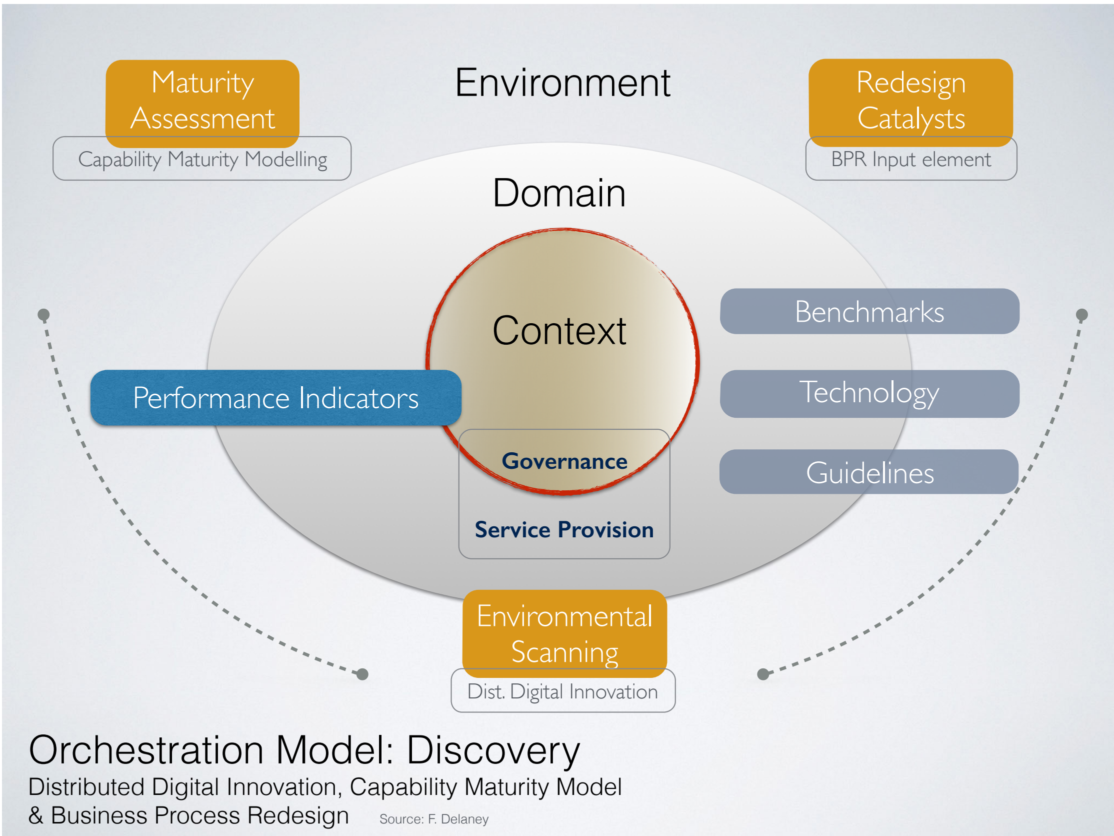

Figure 3.3 Orchestration model of Discovery Phase: DDI, CMM & BPR concepts. Source: F. Delaney.

Two DDI tools are elaborated in the orchestration model shown in Figure 3.3. Three tools (yellow tags) from three different state-of-the-art process re-engineering frameworks are shown contributing to the open innovation view of the context, domain and wider environment.

These tools expose relevant catalyst and performance indicators that describe the context under review. This orchestration model is useful for information and insight gathering purposes. The three state-of-the art frameworks are DDI, BPR and CMM.

There are a number of methods and techniques associated with this model, these are named alongside the stage at which they are utilised.

Phase 1: Discovery

- conduct consultation and desk research (interview, observation, archive research, discussion)
- document context, domain and environment under review (qualitative methods: model context, BPR success framework, capability maturity assessment, BPM risk assessment of blockchain-enabled systems at BFC) **Level 1 multi-level design*
- identify problem-solution design pairings (qualitative methods: creative-thinking techniques); (quantitative methods: blockchain feasibility study of candidate problem-solution design pairings, QSOS evaluation of potential blockchain implementations.) This step concludes with a narrowed selection of candidate solutions. **Level 2 multi-level design.*

Qualitative and quantitative methods are used to analyse the AS-IS services model and extrapolate candidate TO-BE processes in the wild. The discovery phase culminates in the identification of a set of problem-solution design pairings in consultation with process actors in the context under review.

The implementation phase follows an agile development process: scope, design, implement, test and maintain. (This last is out of scope for this research).

Phase 2: Implementation

- describe candidate TO-BE systems with UML: use-cases and proposed architectures **Level 3 multi-level design*
- implement and test feasibility of blockchain-enabled processes
- evaluate implementations (impact and force-field analyses*) *Level 4 multi-level design*

3.2 Multi-level design

The multi-level design technique spans both discovery and implementation phases. This technique offers a semi-structured pathway from current process insights (AS-IS system) towards improved processes (TO-BE systems).

This technique requires the creation of a set of specification outputs, decreasing in their level of abstraction. Together they specify the TO-BE process solution. See Table 3.13 for greater detail.

Multi-level design: expected specification outputs for each of four levels.	
Level	**Output Description**
1	Risk assessment (BPM assessment of 6 core elements) of blockchain enabled systems at Bohemian FC.
2	Problem-solution design pairings arrived at in consultation with process actors at the Club, this process concludes with a blockchain feasibility study.
3	UML and architecture diagrams to specify proposed TO-BE solutions.
4	Assess feasibility of adoption of TO-BE blockchain-enabled processes in the context of the Club (impact and force-field analyses).

Table 3.13 Multi-level design – description of expected outputs at each level.

This approach describes the TO-BE situation at a relatively high level of abstraction, followed by at least two lower levels of abstraction. These together specify the to-be process and are successively considered. An additional level is suggested here in order to select a final candidate system to implement as a demonstration prototype for the research in hand.

- (Level 1 output) BPM risk assessment of blockchain technology solutions at Bohemian FC

As described in Chapter 2, Mendling et al (2017) raise the importance of an organisation developing strategic priorities for any blockchain-enabled process and identifying risks that exist too.

The BPM risk assessment undertaken here assesses the potential impact of blockchain on Bohemian FC service provision. Six core BPM capability areas as described by Rosemann & vom Brocke (2015) include: strategic alignment, governance, methods, information technology, people and culture. This assessment is the first high-level specification of the Multi-level design.

- (Level 2 output) Problem-solution design pairing and blockchain feasibility study

This process arises from the creative-thinking phase of consultation with process actors, as described in section 3.3 Consultation.

Von Hippel and von Krogh (2016) describe dynamic problem–solution design pairing as a temporary matching or an instance of needs, user behaviours, digital artefact features and other socio-technical coincidences.

This process is the second-level specification of the Multi-level design, it concludes with a candidate process selection according to the blockchain feasibility guidelines (Wang et al, 2016). These are described in Chapter 2 Table 2.12.

- (Level 3 output) UML and system architecture diagrams

Unified Modelling Language (UML) is a visual modelling language used in software engineering provide a standard pathway to design and develop a software system. These diagrams represent the third-level specification of the Multi-level design.

- (Level 4 output) Impact assessment and Force-field analyses

In order to determine which proposed solution to showcase as part of this proof-of-concept research an additional Level is introduced to the Multi-level design. This focuses on the impact assessment and factors at play given the context into whether or not the proposed solution would be adopted.

Impact analysis assesses the performance improvement impact and feasibility of proposed TO-BE process alternatives. In this research, the impact assessment describes implications of each proposed solution under five headings: set-up, implementation, consensus protocol, usability and security.

Force-field analysis gives consideration to forces that drive or restrain the implementation of the proposed TO-BE process alternatives.

3.3 Consultation

The purpose of consultation with process actors is two-fold, both relate to the discovery phase of this proof-of-concept research. Firstly, to gather information and insight into the context and AS-IS process systems in place. Secondly, to reveal a set of candidate problem-solution design pairings that may be appropriate for blockchain-enabled process optimisation.

These actors are from within the Context and Domain fields identified in Figure …. Information and insights are gathered through the set of semi-formal interviews, ad hoc discussions, purposeful observation and archival research.

Creative thinking techniques are used to uncover potential process redesign or process innovation candidates: PMI (plus, minus, interesting), visioning and out-of-the-box thinking approaches are to be variously deployed.

A decentralised approach is to be taken to this consultation; process facilitator and process user perspectives are equally valued. Customer and user experiences, in particular, are valued highly. Summary outcomes from the discovery phase are detailed later in this Chapter.

3.4 Documentation

Given that much of the scoping is qualitative in nature, the problem of how to document the research is important.

In order to facilitate a common and thorough understanding of relevant process factors, a bespoke framework, derived from a meta-model of successful business process redesign projects is utilised. This modified framework is titled the BPR success framework.

- **Method: BPR Success Framework**

Adapted from a systematic literature review of successful BPR approaches to system redesign, seven key procedural elements associated with success are itemised and defined (Vanwersch et al, 2016). Six of these elements are relevant here: aim, activity, actors, input, output and technique.

The seventh element tools, refers to team collaboration tools which were not required for this research. For clarity, the framework is briefly described below. Six core elements are categorised, sub-categorised and options are noted. The column on the far-right, labelled PoC (proof-of-concept) indicates whether or not the category was referenced in the current process: * = yes.

The first three fields of the BPR success framework are shown in …. .

First described is the **Aim** field. This field identifies objectives defined either in terms of *Performance dimensions* (revenue, costs, time, quality or flexibility) or *Degree of improvement* (either radical or incremental).

The second field is the **Activity** field. This field fully describes the proposed activity identifying it as either new *design* or existing process *redesign*.

The third field is the **Actor** field. Actors are described as either *Daily Involved* or *Advising*.

In this research context, *Daily Involved* actors include: members of the Executive Board, members of staff and volunteers.

Advising actors include: parents of young players, team members spanning the Club age profile, suppliers and customers.

The role of the researcher is that of an *Advising* support specialist in IT.

BPR success framework (Aim, Activity, Actors).
Adapted from: Vanwersch et al (2016)

Field	Category	Sub-cat	Option	PoC
Aim	*Performance dimensions*		Revenue	*
	(performance measures to be improved)		Costs	*
			Time	*
		Quality	External	*
			Internal	*
			Flexibility	*
	Degree of improvement		Radical	*
			Incremental	*
Activity	*Description*	Process design or redesign		*
Actors	*Daily involved*		Process actor	*
	(executing or managing process)		Management	*
	Advising	Support staff	IT specialist	*
			Customer	*
			Supplier	*
			External consultant	

Table 3.14 BPR success framework: Aim, Activity and Actor.

In Table 3.15, the fourth field of the BPR success model is introduced. This is the **Input** field. It encompasses: *redesign requirements, redesign limitations, AS-IS process specifications, process weaknesses* and *redesign catalysts*.

Redesign requirements includes both Output goals and Stakeholder needs. Output goals (also known as KPIs - Key Performance Indicators) can be internal measurements, external measurements and indications of satisfaction (usually customer, community or peer sentiment). Stakeholder needs are often those identified in a problem description.

BPR success framework (Input). (Vanwersch et al, 2016)

Field	Category	Option	PoC
Input	*Redesign requirements*	Process output goals	*
	(redesign objectives)	Stakeholder / customer needs	*
	Redesign limitations	Constraints	*
	(factors restricting solution)	Risks	*
	AS-IS process specification	Textual process description	*
	(description of current process)	Process model	*
		Simulation model	
	Process weaknesses	Process output measures	*
	(identifying redesign priorities)	Process measures	
		Different opinions: AS-IS	*
		Problem investigation	*
		Culture scan	*
	Redesign catalysts	Guidelines	*
	(inspiration for effective process alternatives)	Previous solutions	*
		Benchmark process insights	
		Benchmark process models	
		Technology developments	*
		Industry value net	

Table 3.15 BPR success framework: Input category and sub-categories.

Redesign limitations encompass *Constraints* and *Risks*. High-level risks and constraints as well as detailed descriptions of factors affecting redesign may be identified here e.g. financial, behavioural or environmental factors.

AS-IS process specifications can be described in text and / or visually modelled. They describe the process currently in place.

Process weaknesses are sub-categorised to include: output measures (KPIs), differing opinions (disagreement about how AS-IS process operates), problem investigation (multi-perspective overview), culture scan (shared values of stakeholders or common ground).

Redesign Catalysts provide the inspiration for process re-engineering. Redesign catalyst sub-categories adopted in this research include: guidelines (e.g. GDPR 2018), previous solutions (internal process optimisations) and technology developments (e.g. distributed technologies).

The fifth field of the BPR success model, shown in Table 3.16 is the **Output** field. It includes: *TO-BE specifications* and *TO-BE assessments.*

BPR success framework (Output). (Vanwersch et al, 2016).			
Field	**Category**	**Option**	**PoC**
Output	*TO-BE specifications*	TO-BE service concepts	
	(process improvements)	Summary redesign proposals	
		Textual process descriptions	*
		Process models	*
		Simulation models	
	TO-BE assessments	Impact analyses	*
	(process alternatives)	Force-field-analyses	*

Table 3.16 BPR success framework: Output category and sub-categories.

TO-BE specifications sub-categories adopted in this research include: process description and process model. *TO-BE assessments* adopted in this research include impact assessments and force-field analyses. These are relied upon in this research to inform decision-making about which processes to adopt.

BPR success framework (Technique). (Vanwersch et al, 2016).			
Field	Category	Option	PoC
Technique	*Unstructured*	PMI	*
	(no pathway from current process insights (as-is) to improvement (to-be), no process alternatives)	Out of the box thinking	*
		Visioning	*
	Semi-structured	Delphi	
	(pathway from current process insights (as-is) to improvement (to-be), but no process alternatives)	Nominal group	
		Multi-level design	*
		Grammar-based	
	Structured	Rule-based	
	(pathway from current process insights (as-is) to improvement (to-be), with process alternatives)	Case-based	
		Repository-based	

Table 3.17 BPR success framework: Technique category and sub-categories.

The sixth field, shown in Table 3.17 is the **Technique** field. This field describes three approaches (*Unstructured, Semi-structured* and *Structured*) to progression from current process insights to concrete improvement ideas and whether or not these are defined alongside new process alternatives.

The Techniques relevant to this research include: *Unstructured*: Visioning, PMI, Out-of-the-box thinking and *Semi-structured*: Multi-level design.

3.5 Conclusion

In this Chapter an overview of the two phase orchestration model used in this research is given. These two phases of orchestration are discovery and implementation both contain three steps.

Phase 1: Discovery

1. conduct consultation and desk research (interview, observation, archive research, discussion)
2. document context, domain and environment under review (model context, BPR success framework, capability maturity assessment and BPM risk assessment of blockchain-enabled systems at BFC)
3. identify problem-solution design pairings (creative-thinking techniques: visioning, PMI). This step concludes with a blockchain feasibility study of candidate problem-solution design pairings.

Phase 2: Implementation

4. describe candidate blockchain-enabled processes with UML: use-cases and architecture
5. implement and test feasibility of blockchain-enabled processes
6. evaluate implementations (impact and force-field analyses)

Spanning these six steps is a multi-level design concept. Multi-level design requires specification outputs at each of four stages throughout this process. These outputs are identified as:

1. risk assessment for introducing a blockchain-enabled system at Bohemian FC
2. problem-solution design pairings, blockchain feasibility study and QSOS evaluation
3. UML and architecture diagrams
4. impact assessment and force-field analyses

Chapter 4 will detail how the research was implemented.

4. IMPLEMENTATION AND RESULTS

4.0 Introduction

In Chapter 4, the proof-of-concept process to identify potential blockchain-enabled use-cases in the wild, follows the orchestration model designed and described in Chapter 3. The two phases of orchestration are followed and the specification outputs of the multi-level design technique are elaborated. The BPR success framework serves as a means of documenting key procedural elements of the orchestration model.

4.1 Orchestration model: discovery phase

The discovery phase includes three steps:

conduct consultation and desk research (interview, observation, archive research, discussion)

describe and model context (BPR success framework, capability maturity assessment and BPM risk assessment of blockchain-enabled systems at BFC)

identify problem-solution design pairings (creative-thinking techniques: visioning, PMI). This step concludes with a blockchain feasibility study of candidate problem-solution design pairings.

4.1.1 Discovery step 1: Conduct consultation

Findings and perspectives were documented according to the BPR success framework. These are summarized below. The participants in the consultation are documented in the **Actors** section. A summary of consultation field research is found in Appendix B.

4.1.2 Discovery step 2: Describe and model context

The context, Bohemian Football Club, is described according to its activities, governance, structural model and field research summary, including interview and observation datasets.

Activities:

First Team

BFC is a professional football club, its senior team participates in the League of Ireland's SSE Airtricity League. The Snr team is ranked 5th for 2017, while the U19, U17 and U15 youth teams each won their League titles this season. The Snr team sponsors are Mr Green, an online gambling company. Snr team players may also benefit from individual sponsorship.

Stadium and Clubhouse

BFC home games have to date been held in Dalymount Park, D7. Dalymount Park has three bars, an online and on-premises shop where merchandise is sold. However, the grounds have recently been sold to Dublin City Council with plans to redevelop it into a state-of-the art football stadium and community leisure centre housing both BFC and League rivals Shelbourne FC. It is a time of upheaval and change as well as new opportunity and optimism.

Youth Academy

Bohemian Youth Academy is said to be one of the fastest growing youth football academies in the city. With a recent injection of strategic staff and funding, youth membership has doubled to over 300 young players in the course of two years. The youth Academy has a stand-alone local sponsor and high-performing youth teams also gain team sponsorship support.

Governance:

Membership organisation

BFC is a voluntary organisation, governed by a voluntary board elected from within its membership. Further to observation and semi-formal interviews with Club members, executives and volunteers, it is observed that the Club's activities are conducted across Sections within the organisation Note: throughout the rest of this Chapter these divisions continue to be referred to as Sections.

Administrative Sections

These Sections operate as silos, with key individuals, staff and /or volunteers operating in each. Ad hoc committees and interest groups are also established to oversee delineated areas of activity, it is a flexible governance model, responsive and resilient in the face of personnel changes and external factors.

AS-IS Structural Model:

The BFC governance model is an example of a distributed management structure with both formal and informal structures and a mix of distinct and indistinct boundaries and roles. Figure is the culmination of qualitative research in order to model the AS-IS system under review at a high-level.

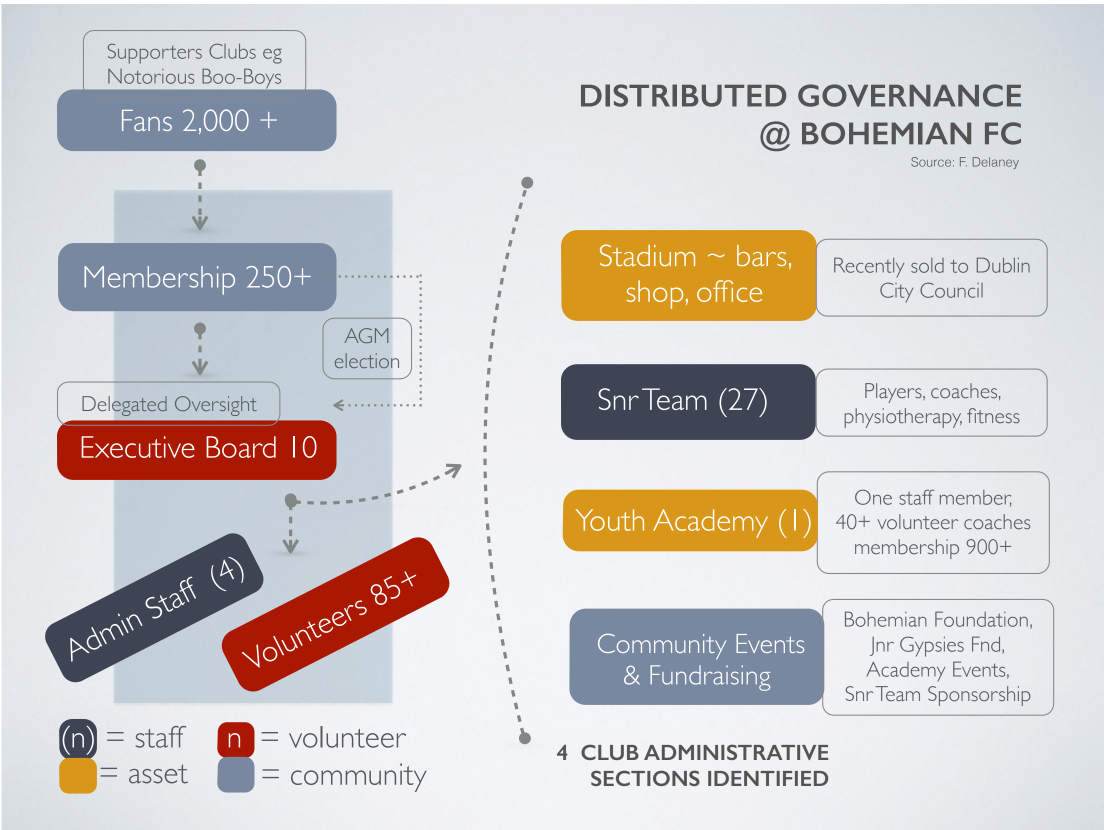

Figure 4.4 Bohemian FC distributed governance model. Source: F. Delaney.

Method: Capability Maturity Model

The Club's activities are assigned a maturity rating according to the Capability Maturity Model. Bohemians FC is considered to be positioned between Stage 1 and

Stage two maturity, with some higher capabilities in select governance fields: elite team oversight and administration is considered to be Stage 5 (optimised); the Youth Academy, undergoing a managed growth process is considered to be between Stage 2 (repeatable) and Stage 3 (defined).

It is clear that business processes can be streamlined with considered strategic approaches and foresight.

Method: BPR success framework

The adapted BPM success model is described in Chapter 3, Tables 3.14 - 3.17. Here, the first three fields: Aim, Activity, Actors and one Input field measure are described.

Aim

The Aim of the re-engineering process identifies Objectives which are either defined in terms of *Performance dimensions* or *Degree of improvement*.

Performance dimensions

In the case of BFC, a high-performance, elite football Club, has many processes to measure success eg. player fitness, team cohesion and team success at the performance level. However, a few internal business processes have applied-performance measures in place. Any process re-engineering effort affords an opportunity to introduce a Club-wide strategy to gather appropriate metrics across these vital channels:

revenue	across income strands and the Sections that deliver the income
costs	across expenses strands and the Sections that accrue expenditure
time	work-cycle and delays
quality	both objective assessment and perception, internal and external, of services/ products delivered. A measure of how flexible the processes are is also useful.

The *Degree of improvement* can be incremental or radical, and will depend on each proposed problem-solution pairing.

Activity

The Activity is identified as any business process optimisation achieved at BFC, through new process *design* or existing process *redesign* and for the purposes of this proof-of-concept research, facilitated by blockchain-enabled technology. These are elaborated in step 3 of the discovery orchestration phase.

Actors

The Actors identified in process re-engineering are described as either *Daily Involved* or *Advising*. In this research context,

1. *Daily Involved* actors include: members of the Executive Board, members of staff and volunteers.
2. Advising actors include: parents of young players, team members spanning the Club age profile, suppliers and customers.
3. The role of the researcher is that of an *Advising* support specialist in IT.

Additionally, outlined here are the common Design catalysts (influential Input dimensions) given the context for process evaluation. These catalysts form part of the Input phase of the PBM success model.

Input

Design / Redesign Catalysts

The over-arching Design / Redesign Catalysts identified for this context include the following three factors:

1. current internal changes and high growth at the Club, in particular the newer Youth & Community Sections
2. data management requirements arising from EU GDPR 2018
3. opportunities afforded by fresh developments in blockchain and distributed technologies

Method: BPM Capability Risk Assessment (Multi-Level output: 1)

A high-level risk assessment of the impact of blockchain technology on business processes at the Club is considered.

A closer look at the six core BPM capabilities reveals the following fields: strategic alignment, governance, methods, information technology, people and culture. Summary findings are found in Table 4.18.

Business Process Management - 6 Core Capabilities identified by Rosemann & vom Brocke, 2015)		
6 core capabilities of BPM and Bohemians FC process redesign with distributed blockchain technology.		
1	Strategic alignment	As a disintermediation process-enabler, blockchain may provide an opportunity to introduce digital traceability into business processes, in a manner that reflects existing governance patterns at the Club. Risk assessment and strategic policies advisable.
2	Governance	The redesign of system processes exposes current governance weaknesses and exposes any conflicts of purpose or section boundary. Actor agency and incentivising participant behaviour are important considerations in a voluntary organisation structure. Process improvements via distributed technologies may alleviate these issues or may reveal a new set of challenges for Club governance.
3	Methods	Exploitative methods used to uncover weakness in existing processes, alongside methods to innovate new processes are a challenge given the current pace of change at the Club and lack of documentation and measurements for existing processes.
4	Information Technology	Blockchain-enabled systems are at the cutting edge of new technology: new trust / threat-models are required. Limitations of distributed technology must be understood in each business use case.
5	People	For BFC to introduce blockchain-enabled systems, additional skills in collaboration, requirements engineering and business analysis are necessary, in addition to the technical skill required to build and maintain the software. There is more likely to be reluctance in adopting new technology than building and managing a new system collaboratively.
6	Culture	In this instance, where the existing system is highly distributed already, the benefits of distributed technology fit well with the culture. It is likely the introduction of strategic business process management may lead to a more resilient organisational culture.

Table 4.18 Risk assessment based on BPM’s 6 core capability fields.

Analysis of the Bohemian FC context under these headings acts as a high-level risk assessment methodology. Consideration is given to how each field may be affected by the introduction of distributed blockchain technology at the Club.

An assumption is made that the existing distributed governance structure at the Club will continue to exist and be supported by the membership / Club owners, staff and volunteers.

Three key points arise:

- Distributed technologies, including blockchain, appear to be a good fit for the organisation's existing distributed governance structure.
- The limited application of strategic optimisation is likely to raise challenges for any process discovery and redesign process.
- The lack of a current IT strategy implies a clean slate in terms of digital innovation. The upside is, there are few barriers to adopting distributed technologies e.g. no legacy license agreements for data storage, software or cloud services. The downside is there is likely to be resistance to business process integration and digital up-skilling.

4.1.3 Discovery step 3: identify problem-solution pairings

Utilising a mix of creative thinking techniques including: visioning, outside-the-box and PMI analyses to evoke a kind of innovation agency.

The researcher sought to discover potential dynamic problem–solution design pairings, described by Von Hippel and Von Keogh (2016) from user needs, user behaviours and other influencing socio-technical considerations.

Method: Problem-solution design pairings (Multi-Level output: 2.1)

Participants were ultimately asked 'If you could improve anything about how things happen here, what would you make happen?'

In this open-ended fashion, nine candidate problem-solution design pairings were identified as problems worth solving with distributed technology. They are summarised in Table 4.19.

Problem-solution design pairings			
Problems identified by Bohemians FC staff, volunteers and other process stakeholders			
ID	Problem	Solution	Source
1	Ongoing need to increase recruits and maintain numbers of volunteer coaches	Streamline the selection and integration process with a data management process	Head Coaches, Youth Committee
2	EU GDPR data management requirements with particular care of data held on children and confidential adult information e.g. Garda Vetting	Introduce GDPR-compliant data-management procedures	Youth Development Officer
3	Players at NDSL level have match play reprimands recorded. These need to be co-ordinated between Club and League	Optimise tracking system for player reprimands on NDSL League teams	Youth Development Officer, team coaches
4	With the growth of the Club's Youth Academy, more kit is distributed to teams, coaches other volunteers, as well as increasing the market for the Club merchandise, no tracking system currently in place.	Introduce Club-wide tracking system for merchandise as its sold or distributed to teams and volunteers	Merchandise Officer, Youth Director, Academy Kit Officer
5	All Football clubs require players (and sometimes parents) to sign behaviour agreements. Coaches too have expected roles and responsibilities to fulfil.	Introduce record of documents as they are signed by parents, players and coaches.	Youth Committee
6	Parents of young players often give poor feedback about communications from the Club.	Introduce quality assurance standards for parent / player communications.	Parents, coaches, Youth Committee
7	When kit is distributed to teams, or sold at pop-up shop events customers are less trusting of the authenticity of the goods than if they get them at the Club shop.	Create proof-of-origin service for merchandise at point-of-sale especially pop-up sales outlets	Academy Kit Officer, Merchandise Officer, customers
8	There is a constant quest for new sponsors of the expanding team-base at the Club.	Streamline the on-boarding process for team and player sponsorship with a crowd-source web-interface	Youth Director
9	Ad hoc design and commissioning of t-shirt stock for the Club shop.	Create voting app for new t-shirt designs to be stocked at the Club shop.	Merchandise Officer, fans

Table 4.19 Nine problem-solution pairings identified in Consultation process.

Method: Blockchain Feasibility Study (Multi-Level output: 2.2)

The problem-solution design parings are assessed for their compatibility with blockchain feasibility guidelines (Wang et al, 2016). Detailed in Table 4.20 and Table 4.21.

PSD Pairings ID 1-9 Source: Blockchain feasibility study (Wang et al, 2016)										
A blockchain solution has strong potential if at least four of the following apply:		1	2	3	4	5	6	7	8	9
1	Multiple parties require views of common data		x	x	x			x		
2	Multiple participants take actions that need to be recorded and alter the data	x		x	x	x	x		x	x
3	Participants need to trust the validity of recorded transactions	x		x		x		x	x	x
4	Disintermediation has potential to reduce cost and complexity									x
5	Reducing delays has business benefits (e.g. enhanced liquidity, lower settlement risk)	x			x	x	x	x	x	
6	Transactions created by different parties depend on each other				x			x	x	
	Total	3	1	3	**4**	3	2	**4**	**4**	3

Table 4.20 Quantitative assessment of blockchain feasibility of problem-solution design pairings.

Problem-solution design pairings: 4, 7 and 8 are identified as having greatest compatibility with blockchain-enabled systems.

Problem-solution design pairings (adapted from Von Hippel and von Krogh, 2016.)		
ID	**Problem**	**Solution**
4	With the growth of the Club's Youth Academy, more kit is distributed to teams, coaches and other volunteers, as well as increasing the market for the Club merchandise, no tracking system currently in place.	Introduce Club-wide tracking system for merchandise as its sold or distributed to teams and volunteers
7	When kit is distributed to teams, or sold at pop-up shop events customers are less trusting of the authenticity of the goods than if they get them at the Club shop.	Create proof-of-origin service for merchandise at point-of-sale especially pop-up sales outlets
8	There is a constant quest for new sponsors of the expanding team-base at the Club.	Streamline the on-boarding process for team and player sponsorship with a crowd-source web-interface

Table 4.21 Three problem-solution design pairings that will progress to implementation phase.

Method: QSOS evaluation framework. (Multi-Level specification output: 2.3)

Blockchain Implementations	**Bitcoin**	**Multichain**	**Ethereum**	**Tendermint**	**Hashgraph**
• Legacy: Project's history and heritage	6	7	6	6	3
• Activity	4	7	4	5	2
• Governance: Project's strategy	6	6	7	6	4
• Professionalisation / industrialisation	6	7	4	4	4
Totals	22	**27**	**21**	21	13

Table 4.22 QSOS evaluation results. (Ref. Chapter 2, Section QSOS evaluation framework)

Table 4.22 shows that the two optimal blockchain implementations selected are Multichain and Ethereum.

At the conclusion of the discovery phase three problem-solution design pairings are selected to move forward to the implementation phase.

4.2 Orchestration model: implementation phase

The implementation phase also has three steps:

Phase 2: Implementation

4. Scope and model candidate blockchain-enabled processes (BPR success framework, UML use-cases and architecture)
5. implement and test feasibility of blockchain-enabled processes
6. evaluate implementations (impact and force-field analyses)

The three problem-solution design pairings that reached the minimum feasibility target of four requirements in the blockchain feasibility study are scoped and implemented here.

Requirements and risks are described using the BPR framework. A high-level risk analysis based on the likelihood of implementation given the context and potential impact is taken and a single candidate process is selected and fully implemented.

4.2.1 Problem-solution design pairing: 1

Internal supply chain traceability of branded Club merchandise. There is no formal cross-organisation tracking system at the moment. This leads to the following difficulties:

- anticipating orders sizes.
- tracking items distributed across Sections.
- mismanagement of credit lines and cashflow across Club sections for orders and payments
- unknown levels of petty theft of goods and cash.

Aim The objectives are described as being achieved across *performance dimensions* and by the *degree of improvement* predicted.

The difficulties noted in the problem description impact upon all five performance dimensions: revenue, costs, time, quality and flexibility. The Aim of this designed solution, internal supply chain traceability, should show a predictable and managed improvement across all five performance measures.

By introducing a traceability feature, reliable process measurements can take place, in turn offering a basis for further strategic growth. Even without a widespread adoption of similar tracking and measurement across business vertices, this represents a *radical degree of improvement* in service delivery according to the BPR framework, as it challenges the organisational framework in its application of new technology.

Activity - *Design*
To design from scratch, a blockchain-enabled internal supply chain traceability system. Each product item represents a system asset with a given quantity to be distributed appropriately across Club sections (Shop, Snr Team, Youth Academy, Volunteers)

before being sold or distributed gratis to teams and volunteers associated with the Club. Club sections are represented by nodes in the traceability system.

Actors

These are identified as *Daily involved* and *Advising*:

- *Daily involved* - process actors: Merchandise Officer, Youth Kit Officer.
- *Daily involved* - process management: Finance Officer, Youth Director, Youth Development Officer and team organisers.
- *Advising* - IT specialist (researcher), customers (players, volunteers), suppliers (Hummel, others).

Input

The Input field of the BPR success model encompasses: redesign requirements, redesign limitations, AS-IS process specifications, process weaknesses and redesign catalysts.

Redesign requirements includes both *Output goals* and *Stakeholder needs*.

Output goals:

Problem-Solution 1: Output Goals, Blockchain-enabled supply chain traceability					
Internal	Definition	How	Frequency	Review	Purpose
cycle-time	Measure of how long it takes assets to traverse the system. (Sum, average, outliers = delay metrics)	Track assets	Weekly	Monthly	precipitate predictability in supply chain mgt.
volume	Measure of how many assets traverse the system through which sections.	Track assets	Weekly	Monthly	as above
External					
output volume	Measure of how many assets are moved out of the system (sold / gratis) and when.	Track assets	Weekly	Monthly	as above
Satisfaction					
Reliability	Customer sentiment relating to service reliability is measured	View complaints, track avg. cycle-time	Weekly	Monthly - (or more often)	Assess negative perception of brand

Table 4.23 Problem-Solution 1: Output Goals, Blockchain-enabled supply chain traceability

Output goals (also known as KPIs - Key Performance Indicators) can be internal measurements, external measurements and indications of satisfaction (usually customer, community or peer sentiment). Shown in Table 4.23.

Stakeholder needs are those identified in the problem description:

- better anticipate future order sizes
- track items distributed across Sections
- determine levels of petty theft of goods and cash relating to merchandise distribution
- improve management of credit lines and cashflow across Club sections in relation to orders and payments

Redesign limitations encompass *Constraints* and *Risks*. High-level risks and constraints have been identified in during the discovery phase. These are summarised in Table 4.18.

Additional *Constraints* for Problem 1 include:

Budget: there is no budget-line from which to fund the system development.
Additional *Risks* include:

Urgency: there may not be an accepted need across Club Sections that such a system is beneficial or offers return on investment. Lack of motivation.

AS-IS process specification A process specification model can be described in text and visually modelled. In Figure 4.5 a system overview is modelled: the supply chain for branded sports apparel and Club merchandise is described. Key actors in the process, both staff and volunteer are noted.

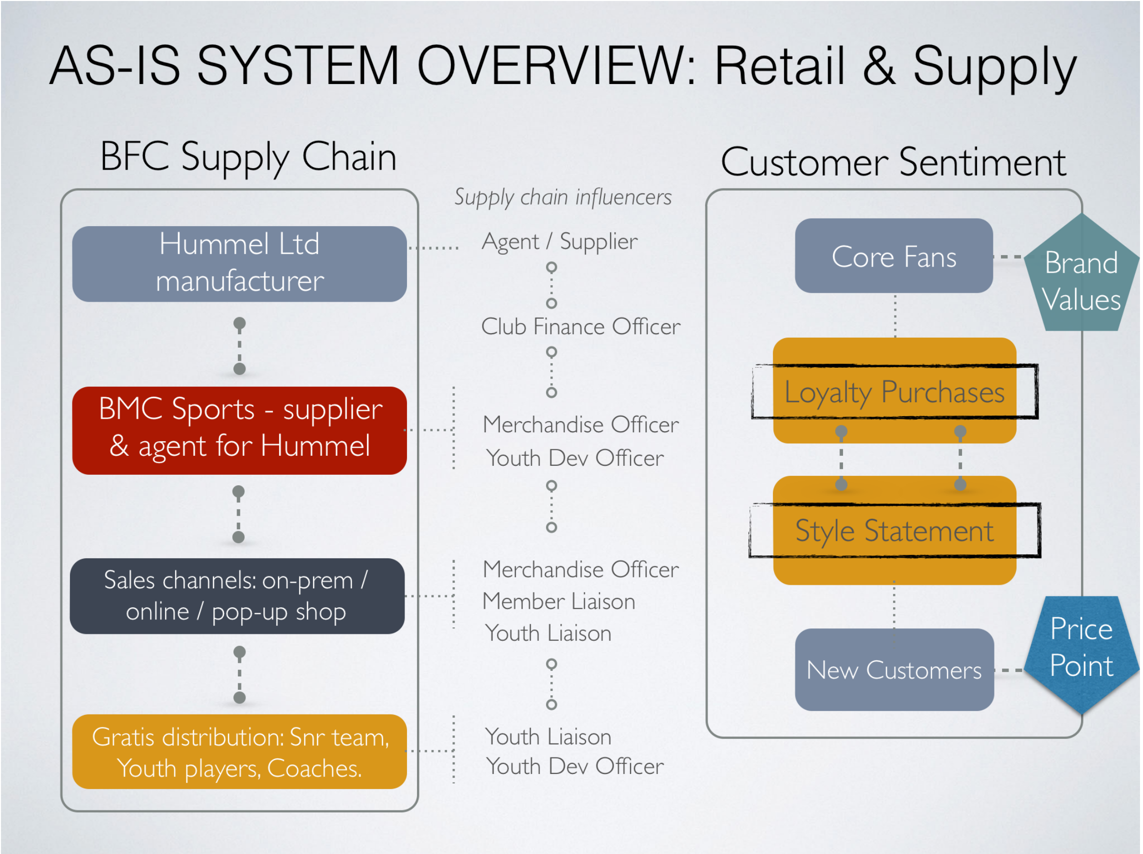

Figure 4.5 AS-IS process specification: supply chain and influencers.

There is no collaboration between Member merchandising section and Youth section. Their budgets are separate and their sales and distribution channels are completely distinct.

Process weaknesses:

Process weaknesses are sub-categorised to include: *output measures, differing opinions, problem investigation, culture scan*.

The current *output measures* in place include tracking sales numbers and managing costs.

In the Youth Section *output measures* are informal: are the players dressed in branded apparel? Is there enough stock for all players (including transfers)? Is anything missing?

Differing Opinions arise between the key Actors in two Sections as to where responsibility should lie for supply management and distribution of apparel.

There is a lack of interest on the part of the Merchandising Section to take on new process requirements. The Youth Section is flourishing, and scaling quickly and has requested the Merchandising Section take over responsibility for distributing Youth apparel and accessories for a youth discount rate. This has been refused.

The *Problem Investigation* sub-category includes information gathering about problems as they perceived by the different process stakeholders.

A process observation of both sales and distribution of free-gratis youth and volunteer kit was undertaken, as were interviews with staff, volunteers and parents at Youth Section. Summary feedback is outlined below:

- There are regular complaints from those seeking to get the gratis kit they need. (coaches / players)
- All Sections suffer from depleted stock and slow re-stock cycles.
- All Sections struggle to anticipate stock requirements in advance of a new season.
- Appropriate process management and metrics would alleviate this situation.

Culture scan is described as requiring an assessment of the shared values of the stakeholders in a process. As noted previously, in this case, there is not a common set of expectations of how the process should operate and who should have responsibility for managing it. The tight control of the Merchandising Section's execution of responsibilities and management of resources (the on-prem shop and online shop) is in contrast to the ad hoc and under-resourced management of the Youth Section's responsibilities. There is a lack of interest on the part of the Merchandise Office to accept responsibility for the burgeoning Youth Section player and volunteer kit requirements.

The shared belief is that each Section is autonomous and responsible for conducting their own business, without help or interference from other Sections.

Design Catalyst

As previously noted three over-arching redesign catalysts are common:

1. current internal changes and high growth at the Club, in particular the newer Youth & Community Sections
2. data management requirements arising from EU GDPR 2018
3. opportunities afforded by fresh developments in blockchain and distributed technologies

In this instance, for problem-solution design pairing: 1, there is an additional catalyst identified:

4. increased internal requirements of staff and volunteers and increased external requirements from young players and their families, and the wider Club community

Output:

The third field in the BPM success model is Output and it has two sub-categories: *TO-BE specifications* and *TO-BE assessments*.

TO-BE specifications proposed are described in the TO-BE system overview in Figure 4.6.

The diagram describes how a permissioned blockchain can support a supply chain traceability system across Club Sections. These Sections act as separate nodes in the system.

The proposal is for a private, permissioned blockchain implementation with total autonomy between administrative Sections in the Club while facilitating asset traceability through the system.

Method: UML use case & architecture model (Multi-Level output: 3)

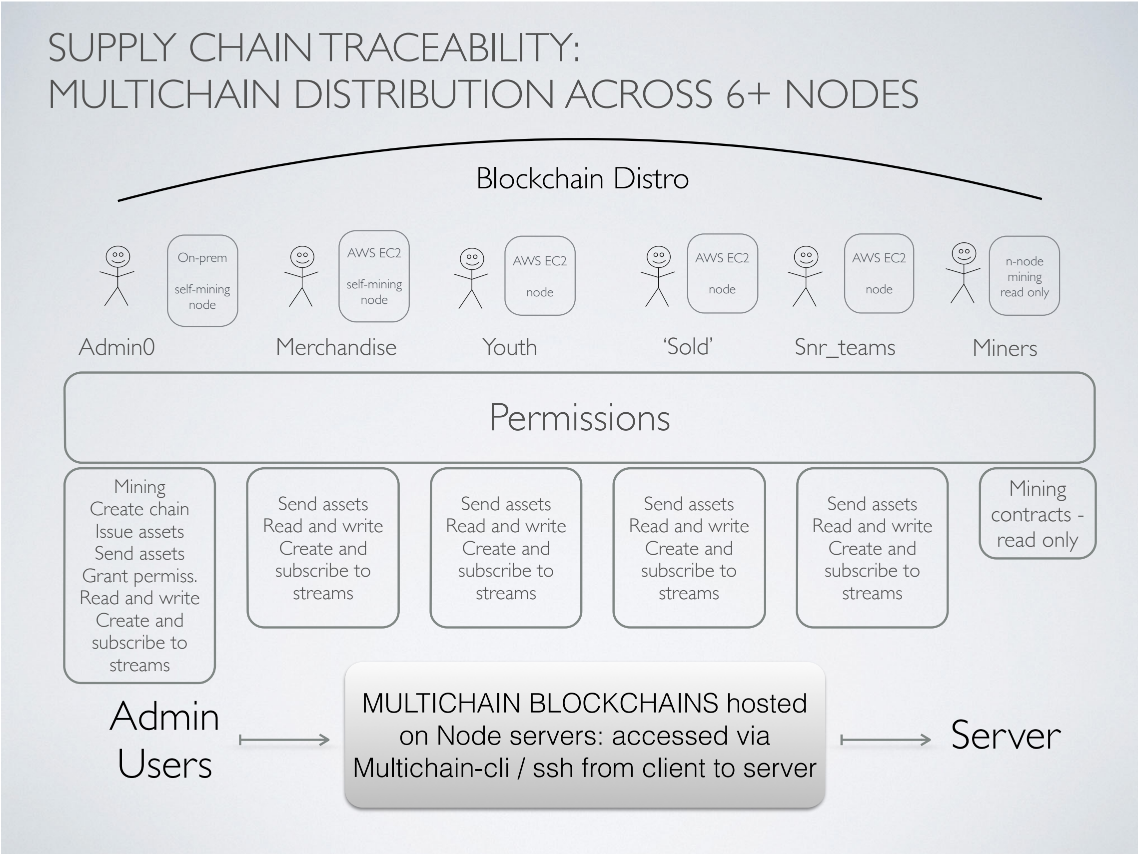

Figure 4.6 TO-BE system specification: product traceability for BFC on permissioned blockchain.

TO-BE assessments are described as being *impact assessments* and *force-field analyse.* These are included in Chapter 5 evaluation section.

This system was tested on a Multichain permissioned blockchain (selected in comparative analysis in Chapter 2) with 6 AWS server nodes and a centralised administrative role to allocate and secure permissions.

AWS offers users a first-year-free offer and this was used to set up multiple server nodes.

A single public blockchain was initiated on which to create and track assets through the system. TO-BE System requirements scoped and designed as per Figure 4.6.

4.2.2 Problem-solution design pairing: 2

The Club is constantly seeking positive sponsorship partners. Currently, Snr team players may be sponsored as individuals as well as benefitting from team sponsorship.

It is currently not possible for the Club community to offer this type of direct sponsorship at a small scale.

Often it is the bookie that benefits from small-scale player interest e.g. Who'll score first goal?

Note: there are restrictions on what types of company can sponsor youth activity (no alcohol, gambling or other inappropriate deals permitted). The youth section remains out of scope for this problem-solution matching.

Aim

The objectives of the activity are described as being achieved across *performance dimensions* and by the *degree of improvement* predicted.

As this proposed system does not currently exist, impacts on all five *performance dimensions*: revenue, costs, time, quality and flexibility are expected and should be measured.

Introducing this sponsorship model may be seen as an incremental *degree of improvement* in the wider sponsorship context in place at the Club.

With the additional responsibility of managing associated social media channels it represents a radical expansion of the quality of player-fan relations facilitated by the Club.

Activity - *Design*

To design an extension of the existing individual player sponsorship model from scratch with a smart-contract enabled crowd-source sponsorship model for individual players on the Snr team. The proposal is to build a crowd-source sponsorship portal for fans and other individuals to sponsor and express support for individual Snr team players. Payments are made in virtual currency tokens, issued on the blockchain. Typically these types of crowd-funding relationships are offered in tandem with bonus feature type content for sponsors via social channels (eg Instagram, YouTube).

Actors

These are described previously and include: Club fans and Members of Snr team.

Problem-Solution 2 is further mapped according to the Input field of the BPM success model: redesign requirements, redesign limitations, AS-IS process specifications, process weaknesses and redesign catalysts.

Redesign requirements

These encompasses both *Output goals* and *Customer / Stakeholder needs.*

Output goals (KPIs) are internal or external measurements, or indication of satisfaction (usually customer, community or peer sentiment). They are summarised in Table …. .

Redesign Limitations:

Redesign limitations encompass *Constraints* and *Risks.* High-level risks and constraints have been identified in Table 4.24. Additional Constraints for problem-solution pairing 2 include:

Budget: there is no budget-line from which to fund the system development.

Additional Risks include:

Negative User Behaviours: this solution assumes that players receiving individual sponsorship in this way, is a positive thing for them and the team. Managing sponsor expectations may outweigh the benefits of their support. It may introduce a distracting degree of intra-team rivalry between players.

Problem-Solution 2: Output Goals, Crowd-sourced individual sponsors for Snr team players					
Internal	Definition	How	Frequency	Review	Purpose
cycle-time	Measure of how long it takes to onboard a sponsor and how long they remain in the system	Track sponsorship	Weekly	Monthly	Measure success, look for triggers to system exit
volume	Measure of how many sponsors join, remain and leave the system	Track sponsors	Weekly	Monthly	as above
External					
error rate	How the system is treated and responds to process handling	Logging	Weekly (or more often)	Weekly (or more often)	maintain and optimise web-service
income	How much additional sponsorship acres	Track sponsorship	Weekly	Monthly	Measure success, look for triggers to system exit
Satisfaction					
Responsiveness	Sponsor sentiment towards the players and to the rewards they receive for their support	View comments/ complaints, track avg. cycle-time	Weekly	Monthly - (or more often)	Assess perception of Club and player personal brands

Table 4.24 Problem-Solution 2: Output Goals, Crowd-sourced individual sponsors for Snr team players

AS-IS process specification:

The Club currently offers individuals and businesses the opportunity to sponsor the home and away jerseys of individual players on the Snr Team: home jersey costs €300, away jersey €250, and to sponsor both costs €450. The player sponsors are stitched into the players' jerseys. This is paid for through the online shop and is facilitated on a first come first serve basis.

The Club recognises the relationship in player details in each match program. Sponsors are also invited to a meet-and-greet on match nights.

The Club doesn't offer its community direct sponsorship at a smaller scale nor officially facilitate social media relations between players and fans.

It would appear that, for the most part existing fans of the Club form the core of player sponsorship deals: there are 31 sponsors listed for players and coach of these, 9 are named businesses, the rest are named fans or fan clubs e.g. Woodstown Bohs, The Hut Bohs, Gay Bohs.

The Club is only actively involved in seeking team and Club sponsorships, not individual player deals, which seem to manage themselves.

Process Weaknesses:
Process weaknesses are sub-categorised to include: *output measures, differing opinions, problem investigation, culture scan*.

Output Measures (AS-IS):
Revenue incoming, expenditure outgoing. No other success metrics identified.

Differing Opinions
Snr Team players appreciate the current support model and enjoy meeting sponsors at the meet and greet.
Some Snr Team players feel the process could be scaled up and find the proposal an exciting opportunity while others find it potentially distracting. Would it be part of their existing contracts to participate or would it be voluntary?

Fans often like to take a gamble on individual players and team performance, is there potential to maximise on this interest? Some feel that a gamified or performance betting version might be more interesting than a straight forward crowd-funding model.

The proposal offers a potentially larger number of fans to support and to interact with their favourite players. This is seen by some as positive and by others as negative.

Problem Investigation This sub-category includes information gathering about problems as they are perceived by the different process stakeholders.

Technology context:

Ethereum is a public blockchain built to support the execution of smart-contracts. It charges 'Gas' as transaction fees and has its own virtual currency, which is publicly traded called Ether. This volatility is not an attractive aspect of Ethereum's platform for enterprise development.

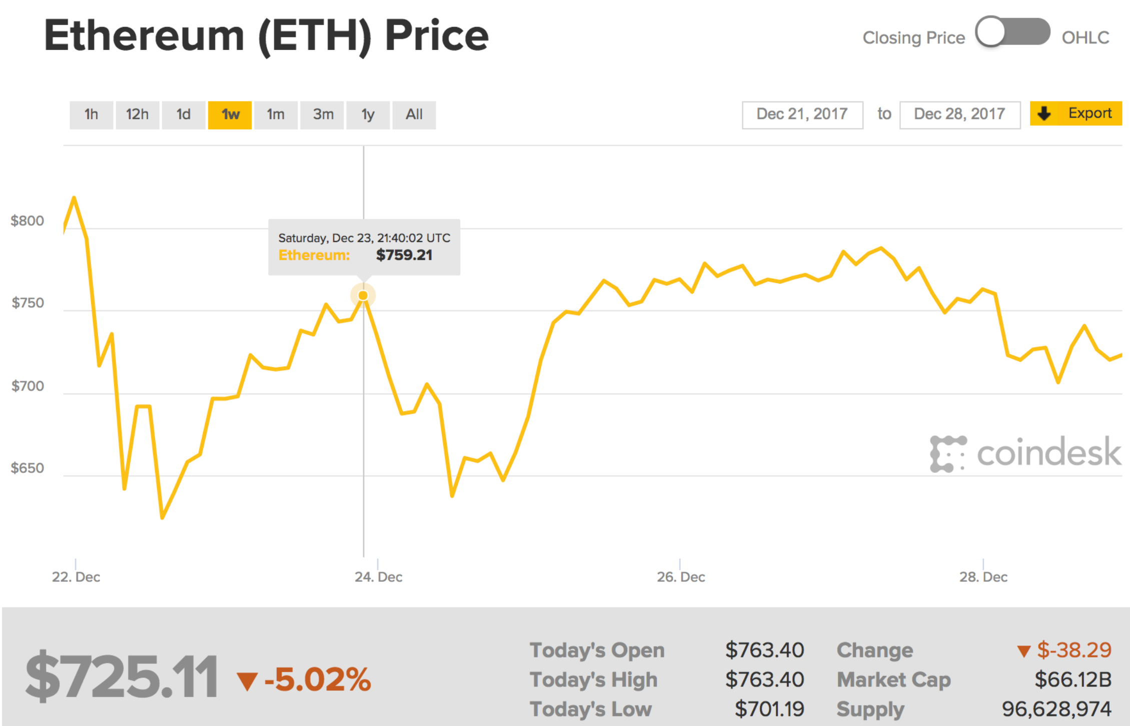

Figure 4.7 shows the volatility of Ether during the week of 21-28th December 2017.

(Source: coindesk.com/ethereum-price/)

Club Context:
Interviews with players, executive board members and adult fans were held.
All interviewees see this proposition as a departure from existing sponsorship models and is seen largely as a monetised marketing proposition.

While there are precedents for crowd-funding individual athletes in cycling, judo and athletics, there is no precedent for crowd-sourcing direct sponsorship for members of the same team, as far as is known.

Culture Scan it seems that while fans often bet on team and player outcomes they mostly do this for their own interest and enrichment, it does not necessarily translate into an interest in funding players directly for “a few extra YouTube videos and a Christmas Card” (a fan).

No one shared any familiarity with using virtual currencies, virtual wallets or interacting with DApps.

Design Catalysts are identified
(1) opportunities afforded by fresh developments in blockchain and distributed technologies, in particular smart-contracts written on the Ethereum blockchain
(2) broader acceptance of the crowd-funding model of support

Output:
The third field in the BPM success model is Output and it has two sub-categories: *TO-BE specifications* and *TO-BE assessments*.

The proposed TO-BE system specification overview describes how a smart contract on the public Ethereum blockchain can be deployed to implement a ‘Team’ factory and ‘New Player’ sponsorship contract which send and receive ERC20 tokens (virtual currency) as a means to crowd-funding individual player sponsorships.

Method: UML use case & architecture model (Multi-Level output: 3)

This system was modelled in a two-step smart-contract interaction on Ethereum. A Team factory smart contract was crafted for the EVM in Solidity language, to allow the Club to create a new team set-up each season and after the Transfer window. Players can be added, removed and Sponsors can be registered, make payments and can have payments returned (a cautious addition to protect brand reputation in the case of mistakes). Only the Club can withdraw funds on behalf of players.

Ethereum Virtual Machine language, Solidity is used to draft a smart-contract factory which produces individual smart-contracts, accessible to the public on Ethereum blockchain (testnet at the moment).

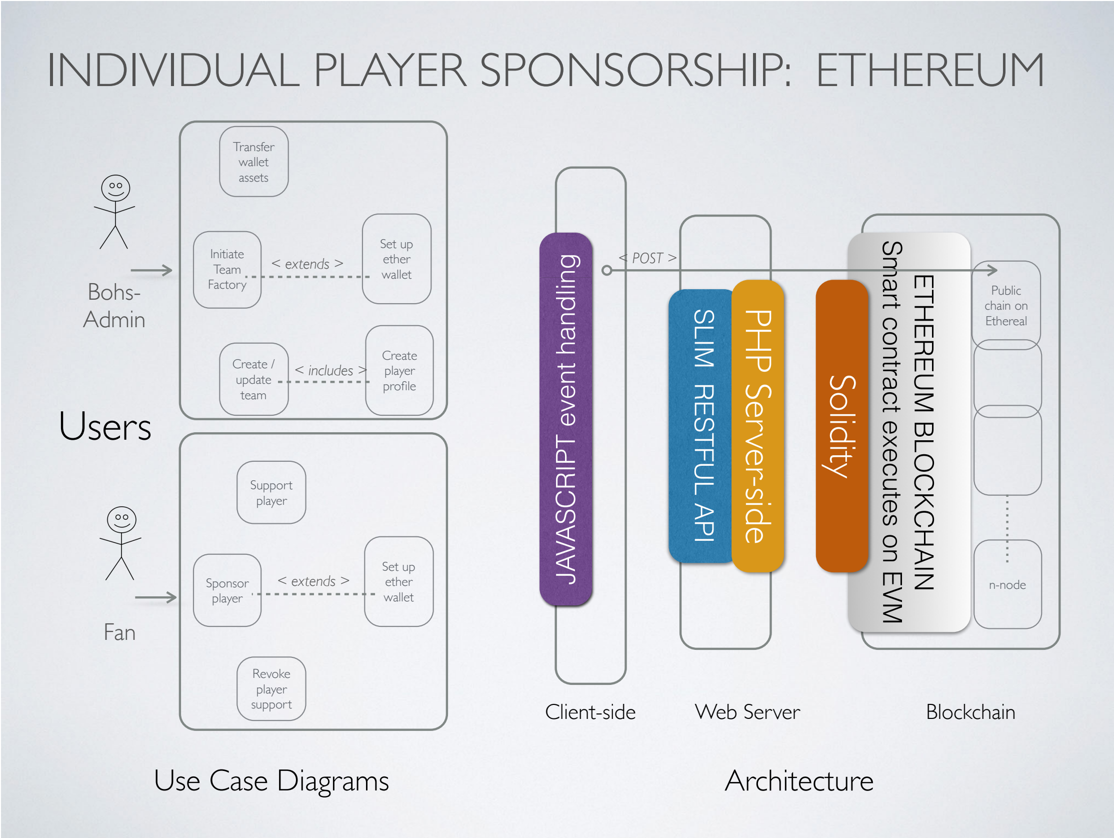

Figure 4.8 TO-BE system specification: crowd-fund sponsorship model on public Ethereum blockchain.

The DApp is owned by the Developer, managed by the Club and interacted with by Sponsors (who have access to a Web3 enabled ether crypto-wallet).

The contract introduces features which allow the Owner/Developer to amend errors and provide security to the proposed application. This is a test protocol for the moment, those powers may be transferred to the Club in a deployment environment.

Truffle IDE includes a testing framework and Ethereum provides a public testnet to test applications in real life without deploying to production mode. This system was tested on the public Ethereum testnet blockchain (selected in comparative analysis in Chapter 2) by installing Go-ethereum (Geth) onto Mac Book Pro X machine. The testnet allows for DApp and smart-contract deployment in a sandbox environment without transaction fees.

TO-BE assessments are described as being *impact assessments* and *force-field analyses*. *Force-field analyses* are included in Chapter 5 evaluation section.

TO-BE System requirements scoped and designed as per Figure 4.8. The public blockchain was synchronised with the Core and a coinbase was mined in order to cover any costs associated with testing.

4.3.1 Problem-solution design pairing: 3

Blockchain enabled proof-of-origin web-service available at point of sale to potential customers. Sportswear is often subject to counterfeiting. Football apparel is often pirated. This is known as brand piracy or theft of brand IP.

- It’s possible, likely even, that outside of the Shop outlet, low-level theft of stock occurs given current lack of stock management and traceability
- Customers who knowingly buy counterfeit goods don’t care if goods are fake
- Beneficiaries are brands and customers tricked into buying fake gear
- Consumers benefit from enhanced trust in supply
- Brands benefit from enhanced Customer Relationship Management

Aim

The objectives are described as being achieved across *performance dimensions* and by the *degree of improvement* predicted.

The difficulties noted in the problem description impact upon three of five performance dimensions: revenue, perceived quality and flexibility. The Aim of this design solution should show a predictable and managed improvement across three performance measures.

This is a brand new, marketing-based value proposition that represents an expansion of consumer trust models. This represents a radical process improvement.

Activity – *Design*

To design from scratch, a smart-tag system, providing anti-counterfeit proof-of-origin via mobile web-app for consumers at point-of-sale.

Using a permissioned blockchain framework to build a secure, immutable, time-stamped record of merchandise assets. This use case expands on one of the only widely adopted blockchain use cases outside of crypto-currency: proof-of-existence notarisation.

The smart-tag, anti-counterfeit web-app is deployed on a Multichain blockchain with a Javascript front-end and PHP backend. It facilitates the deployment and querying of smart contracts to issue verifiable, proof-of-origin transparency to the purchasing process.

Actors

These are identified as *Daily involved* and *Advising*:

- *Daily involved* - process actors: Merchandise Officer, Youth Kit Officer.
- *Advising* - IT specialist (researcher), customers (players, volunteers), suppliers (Hummel, others).

Problem-Solution 2 is further mapped according to the Input field of the BPM success model: redesign requirements, redesign limitations, AS-IS process specifications, process weaknesses and redesign catalysts.

Redesign requirements:

Redesign requirements include both *Output goals* and *Customer / Stakeholder needs*.

Output goals (KPIs): internal and external measurements or indications of satisfaction (usually customer, community or peer sentiment). These are detailed in Table 4.25, on p. 28.

Redesign Limitations:

Redesign limitations encompass *Constraints* and *Risks*. High-level risks and constraints have been identified in Table 4.18. Additional *Constraints* for problem-solution pairing 3 include:

Budget: there is no budget-line from which to fund the system development.

Additional *Risks* include:

Need: this is a novel system. It is difficult to define and measure return on investment. The proposed concept was tested with a simple QR tag and a html webpage, to see if customers could or would be interested to use the system. https://fgdel.github.io/

A high-level consumer survey was also conducted to gather feedback on the concept and determine who would pay to use the service. 65% of those surveyed identified that consumer trust was important enough of an issue for them to consider paying for it. 70% agreed that enhancing consumer trust is a problem in retail: provenance, quality, health and safety concerns e.g. pharmaceuticals, and worker conditions were all identified as contributing to consumer trust deficits.

Problem-Solution 3: Output Goals, Blockchain enabled proof-of-origin web-service					
Internal	Definition	How	Frequency	Review	Purpose
cost	Costs averaged over annual use: staff time, marketing content creation, system maintenance.	Track sponsorship	Monthly	Annual	Return on Investment assessment
volume	Measure system use by volume, compared with purchases.	Track use and sales	Monthly	Annual	Ascertain patterns of use
External					
error rate	How the system responds to process handling	Logging	Weekly (or more often)	Weekly (or more often)	maintain and optimise web-service
Satisfaction					
Assurance	Analyses of perceived trust in BRC brand.	Track comments/ complaints, interview users	6-monthly	6-monthly	Assess perception of Club brand

Table 4.25 Problem-Solution 3: Output Goals, Blockchain enabled proof-of-origin web-service

AS-IS process specification:

The Club addresses consumer trust in the following ways:

- restrict supply to trusted parties: e.g. shop, coaches,
- rely on high-brand recognition: BFC, Hummel and Mr Green,
- product tagging: Hummel product tags are used, not additional BFC tags

In Figure 4.9 the context of customer sentiment towards the purchase of branded goods is described at a high-level. It identifies that core fans are influenced by club loyalty and brand values and expect to see these reflected in their purchases.

On the other hand, new customers are more likely to be affected by style and price point. Their purchase is a de facto introduction to BFC brand values.

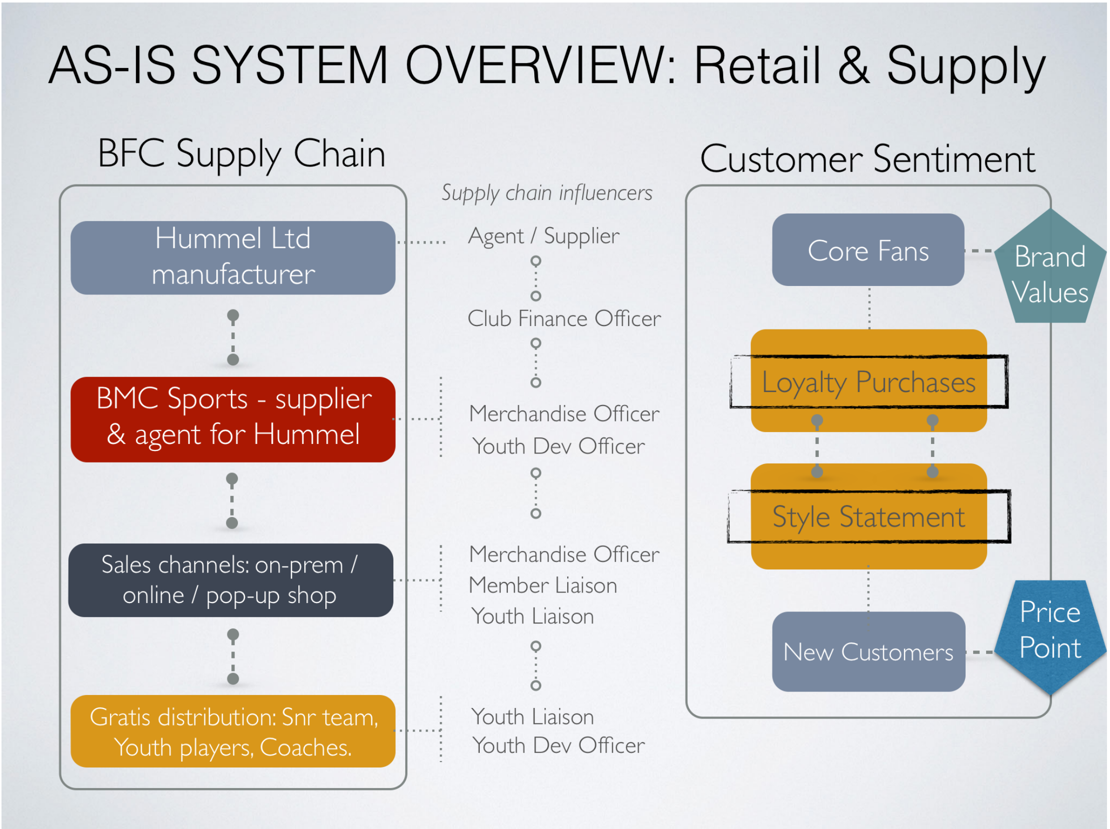

Figure 4.9 AS-IS process specification: customer sentiment and consumer trust

Process Weaknesses:

Process weaknesses are sub-categorised to include: *output measures, differing opinions, problem investigation, culture scan*.

Output Measures (AS-IS):

The only measure of customer sentiment towards the products is whether or not they are bought. Customer sentiment is affected by Snr team performance; there are notable increases in sales when the Snr team performs well.

Product popularity is also affected by the perceived stylishness of the merchandise. The Club association with Hummel has proven to be a popular one.

Differing Opinions:

Representatives within the Club and external to the Club are positive towards the idea. Retailers, customers, business owners, fans, Club officers and volunteers.

It is largely seen within the context of marketing, brand enhancement and customer relationship management. Return on investment is difficult to quantify. Everyone says they'd happily use the system - but aren't interested in paying for it. e.g. Customers won't pay to download an App, just to scan BFC products.

Problem Investigation:

This sub-category includes information gathering about problems as they perceived by the different process stakeholders. Consumers are widely affected by trust issues in relation to their purchases: sportswear in particular is subject to much brand piracy. This proposal seeks to address an issue that is current in the wider environment and apply it to a problem, that conceptually at least, every brand experiences: consumer trust is an aspect of brand perception.

IP counterfeiting in a global, networked context:

A brand's identity is considered Intellectual Property (IP) and IP-intensive industries are targets for criminal enterprises and counterfeiting. Intellectual Property Rights (IPR) infringements are global industries. IPR infringements widely occur in the EU, where manufacturing counterfeit goods and importing counterfeit labels has increased. (Joint Report Europol/Euipo Situation Report on Counterfeiting and Piracy in the European Union, 2017).

Interviews with customers, retailers, Bohemians Merchandise Officer:

At BFC, as described elsewhere, the sale of merchandise is tightly controlled on premises. Merchandise Officer sees no real need for an enhanced trust feature for customers as all the members trust her, in the shop. Note: the Club will move from the Stadium during redevelopment, the shop and building resources will be out of bounds. The sales on match nights will likely be curtailed, by virtue of matches not taking place in Dalymount Park.

Currently, customers and recipients of product free gratis youth and volunteers, often experience delays in getting goods. This negatively affects customer sentiment. Improving the flow of product through the system was an aim of Product-solution 1 it is out of scope here. The point however raises the fragility of consumer sentiment towards a brand.

Culture Scan:

All parties agree it is a marketing and brand enhancement initiative.

Design Catalysts are identified :

(1) opportunities afforded by fresh developments in blockchain and distributed technologies, in particular the enhanced public trust features afforded by blockchain datastores,

(2) expanding market for services that address anti-counterfeiting in branded retail.

Output:

The third field in the BPM success model is Output and it has two sub-categories: *TO-BE specifications* and *TO-BE assessments*.

Figure 4.10, p. 82, describes how admin users register data on a publicly accessible, permissioned blockchain and how potential customers scan a smart tag with their with mobile device and access a proof-of-origin web-service.

This proposed system was tested on a private Multichain blockchain with two AWS servers.

The publicly accessible Node-2 was set up as the public-read-only Node and the primary Node set up as the Admin Node, creating assets and issuing updates using the unique Stream feature of Multichain. This facilitates a 2MB data limit on transaction size and enhanced record and retrieve functions.

Free to use QR code create and readers were used to create the smart tag web-link between mobile reader and publicly accessible blockchain on public Node 2.

TO-BE System requirements scoped and designed as per Figure 4.10. A single publicly accessible, read-only access blockchain was initiated on which to verify the proof-of-origin of Bohemian FC assets to customers at point-of-sale.

Method: UML use case & architecture model (Multi-Level output: 3)

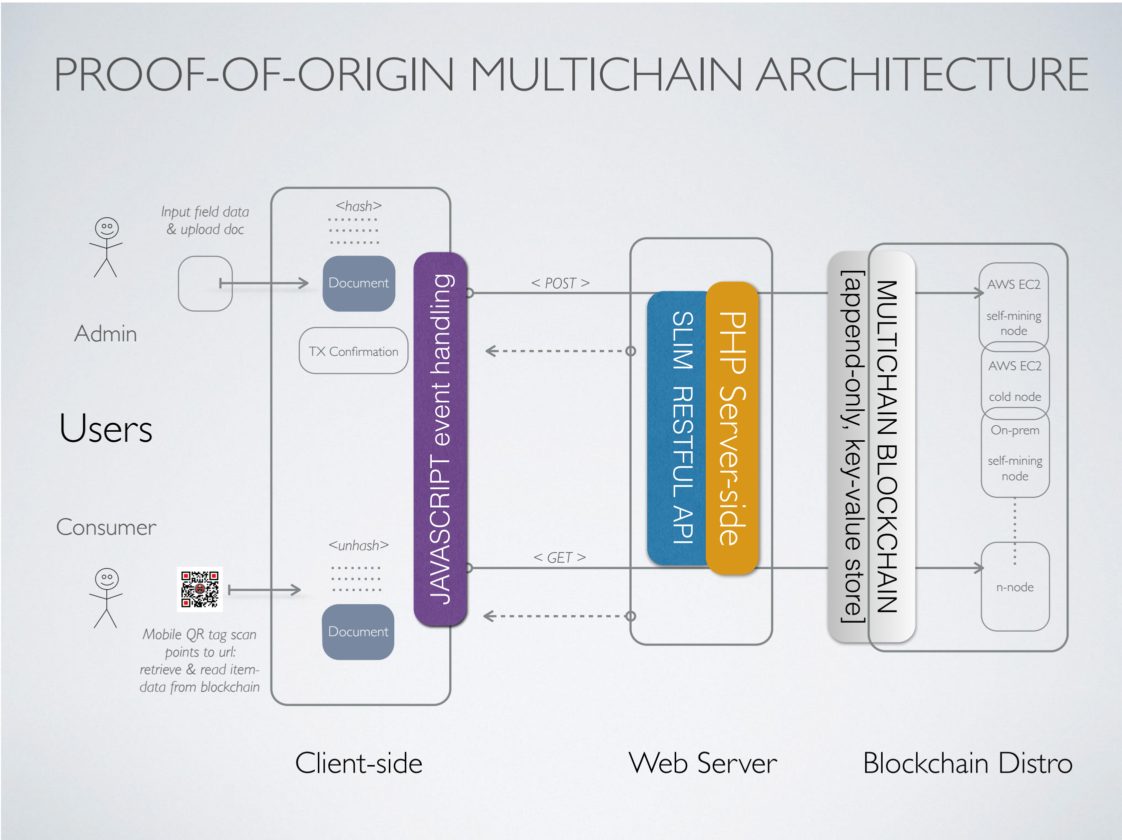

Figure 4.10 TO-BE System overview: Use Cases and proposed web-architecture.

TO-BE assessments are described as being *impact assessments* and *force-field analyses* of the proposed new processes. These are included in Chapter 5 evaluation section.

This system was tested on a permissioned Multichain blockchain (selected in comparative analysis in Chapter 2) with 2 AWS server nodes: one public, read-only accessible to the web interface and one admin server to initiate the root chain and write information to the blockchain using Multichain Streams transaction feature.

4.3 Multi-level design specification outputs

Multi-level design is a semi-structured technique that offers a pathway between current AS-IS system towards an improved TO-BE process in the future.

There are three levels of process and / or context abstraction with a final evaluation of implementations in Level 4.

The specification outputs of this multi-level design are summarised below.

Level 1: Blockchain risk assessment at Bohemian FC (Table 4.18)
Level 2: Problem-solution design pairs (Table 4.19) and Blockchain feasibility assessment (Table 4.19)
Level 3: UML use case & architecture models (Figure 4.6, Figure 4.8, Figure 4.10)
Level 4: Impact assessment and force-field analyses. (Chapter 5; …., …., ….,)

4.4 Conclusion

In this Chapter the implementation of the two-phase orchestration model described in Chapter 3 is documented. Documentation follows the six key procedural elements identified in the BPR success framework.

In order to successfully innovate new business use cases in the wild, scoping context capabilities are an important aspect. The orchestration model and Multi-level design technique and BPR success framework have successfully guided the research to identify a set of implementable blockchain-enabled systems at Bohemian FC. The research design is considered a success.

Findings and outcomes are evaluated and discussed in Chapter 5.

5. ANALYSIS, EVALUATION AND DISCUSSION

5.0 Introduction

Chapter 5 affords an opportunity to review the research undertaken, identifying and giving consideration to what is revealed through the process.

Firstly, an evaluation of the methodology reveals the strengths and weaknesses of the approach. The evaluation includes: the two phase orchestration model, the multi-level design technique deployed to drive the process from current to potential future systems and the backbone of the research strategy, the modified BPR success framework is considered.

Blockchain technology is considered from a maturity perspective, private permissioned and public blockchains are discussed and the role of cryptography in implementation is examined. Areas for future study are also identified.

5.1 Evaluation

5.1.1 Orchestration model

In order to identify and test potential blockchain use-cases in the wild an open innovation strategy was adopted. Akin to the ideation phase of an industrial design process, the two-phase orchestration model was designed in order to reveal as many potential use-cases as possible for deployment in a real-world context: Bohemian FC.

The orchestration model offers a qualitative iterative, distributed modelling process informed by DDI, BPR and CMM frameworks, to scope appropriate blockchain-enabled process improvement at Bohemian FC.

The model succeeds in its aim to reveal as many potential use-cases as possible for deployment in a real-world context: identifying nine problem-solution design pairings, from which three met the feasibility criteria for blockchain enabled systems.

This is considered to be an abundant outcome and may suggest there is lack of digital innovation approaches currently being undertaken to discover blockchain use cases.

The weakness in the model stems from its strength: flexibility and fluid boundaries. Without a keen understanding of the frameworks and tools involved, another person following the model may deploy them differently with different results.

There are two phases in the orchestration model:

Phase 1: Discovery

1. conduct consultation and desk research (literature review, interview, observation, archive research, discussion)
2. document context, domain and environment under review (BPR success framework, model context, capability maturity assessment and BPM risk assessment of blockchain-enabled systems at BFC)
3. identify problem-solution design pairings (creative-thinking techniques: visioning, PMI). This step concludes with a blockchain feasibility study of candidate problem-solution design pairings.

Analysis of the existing context and speculating about possible future systems in an open and unbounded fashion allowed the researcher to explore multiple innovation approaches. Given a different setting the approaches, techniques and tools may indeed have been different.

This flexible approach relied upon a mix of qualitative (creative thinking methods and multi-level design) and quantitative assessments (QSOS evaluation model and the blockchain feasibility study) to compare problem-solution design pairings that arise from the discovery phase.

Phase 2: Implementation

4. describe candidate blockchain-enabled processes with UML: use-cases and architecture
5. implement and test feasibility of blockchain-enabled processes
6. evaluate implementations (impact and force-field analyses)

The implementation phase for each of three identified use-cases was swift and closed-ended, following a waterfall model of software development. This is not necessarily how a production-level implementation of a new blockchain-enabled system would or should occur.

However, in the spirit of maximising potential use-case insights, three implementations were scoped and built quickly in order to facilitate the research process.

The conclusion of the implementation phase examines each use case in the context of the Club and makes a determination about whether or not it would likely be deployed.

These are implementation evaluation tools built into the orchestration model via the multi-level design technique.

Problem-solution 1 – Supply Chain Traceability

This system was tested on a Multichain permissioned blockchain (selected in comparative analysis in Chapter 2) with 6 AWS server nodes and a centralised administrative role to allocate and secure permissions. AWS offers users a first-year-free offer and this was used to set up multiple server nodes.

A single public blockchain was initiated on which to create and track assets through the system. TO-BE System requirements scoped and designed as per Figure 4.6.

Method: Impact assessments (Multi-Level output: 4.1)
These are summarised in Table 5.26.

Impact assessments: **Outcomes of Test Phase: Problem-solution 1**

Topic	Description	Time	Quality	Support	Comment
Set-up	6 AWS servers Apache2 Ubuntu 16.4 Multichain 2.0 preference installations unique PKI Certificates	2 days	resilient, redundant, secure.	Wide community support for all set-ups	A fair degree of technical know-how required to set up servers and install all dependencies: some personalising and tweaking defaults required.
Implement	tweak the design and implement the permission system, asset structure and distribution model	5 days	Robust though inflexible - arising from immutability.	How-to do things is clearly sign-posted in Multichain FAQ	Absolute visibility of asset movements along a timeline is an excellent facility in this context. Mistakes cannot be corrected - given the use case, distributed governance + limited IT skills, this is problematic.
Consensus	Proof-of-work with a low difficulty setting for private chain. Little energy wasted on processing. No transaction fees.	ongoing - across mining nodes	Excellent	FAQ	Consensus is achieved almost instantly and block confirmation occurs within a 15 second timeframe. (This can be tweaked). Each connected node is updated within the 15 second window.
Usability	CLI interface and Multichain Explorer GUI	1-2 hours to learn	Not really accessible An admin or sales person may struggle with these interfaces.	Commands available on Multichain website and in Help command	The CLI interface is simple to use and easy to understand for a technical person. The Explorer GUI is functional and simple to use. A bespoke interface would be useful, to simplify and declutter the interface.
Security	PKI SSH to servers / nodes. Permissioned access to nodes via Admin Server. Permissioned roles according to responsibilities.	ongoing	System is only as robust as its users: training + motivation.	Requires oversight. Identified as being that of Admin Node.	Nodes must secure access points, otherwise it's easy to spoof user ID. Mistakes are easily made regardless of technical ability: no roll-back feature.

Table 5.26 Outcomes of Test Phase for Problem-Solution 1: supply chain traceability system.

Method: Force-field analysis

Force-field analyses are investigations of forces that drive or restrain the implementation of new or re-engineered processes.

In this instance, given there is little to no traceability in the current system, a most basic assessment would suggest this proposal is a welcome improvement.

However, there are likely to be a number of up-skilling and other challenges to address in order to adopt the proposed system. Multiple parties are required to participate in the system.

As each node represents a Section in the Club's structure that has responsibility for distributing apparel, each node must designate a role for updating the system.

Currently, key administrative roles across most Sections are ad hoc and many are vacant. The proposed implementation requires a consensus across administration boundaries and currently there is no system in place to achieve this.

Conclusion: problem-solution 1
It is unlikely this system would be adopted, given the current governance structure and the technical requirements of the implementation.

Problem-solution 2 – Crowd Sourced Player Sponsorship

TO-BE System requirements scoped and designed as per Figure 4.8.

The public Ethereum blockchain was synchronised with and a coinbase was mined in Geth which would cover the 'Gas' for transaction costs.

In the end, as the smart contracts were deployed on the testnet, no Gas costs were incurred.

Method: Impact Assessment (Multi-Level output: 4.1)
These results are summarised in Table 5.27.

Impact assessments: **Outcomes of Test Phase: Problem-solution 2**

Topic	Description	Time	Quality	Support	Comment
Set-up	Install Geth, Solidity EVM, allocate threads to mine coinbase	30 mins to install, 6 days to synchronise to Core.	redundant and fail-safe once connected to Core.	Wide community support for all set-ups	Some technical know-how required to set up and install all dependencies.
Implement	Solidity, one of three languages compatible with EVM was used to write the smart-contracts.	5 days	They contracts are not elegant, but worked in pragma on the testnet.	Plenty of Solidity tutorials available	The unpredictability of how users will interact with the system is a concern. It's not possible to conduct adequate tests without actually setting up the contracts. Testing would have to be live. Risky for a well-known brand.
Consensus	Proof-of-work, high difficulty, energy inefficient.	across all connected nodes	OK, if the network is not clogged by spawning Cryptokitties	FAQ	Consensus is achieved in up to 3 mins on the testnet depending on contract size and complexity.
Usability	CLI interface and testnet GUI	3-4 hours to learn	Need to be a developer to write smart-contracts	available in help commands, and on website	The CLI interface is simple to use understand for a technical person. The testnet GUI is functional and simple to use. A bespoke user interface required: HTML, javascript
Security (of smart-contract not web-interface)	PKI authentication Permissioned roles Wallet security user's concern.	ongoing	System is only as robust as its users: training + motivation.	Requires admin oversight. Technical skills needed.	Smart-contracts need to be executed in the same way at each node. No guarantee that happens.

Table 5.27 Outcomes of Test Phase for Problem-Solution 2: smart-contract crowd-sourced sponsorship

Method: Force-field analyses

Force-field analyses are investigations of forces that drive or restrain the implementation of new or re-engineered processes.

In this instance, there are likely to be a number of up-skilling and other challenges to address in order to adopt the proposed system.

Player participants most likely to benefit are those early-adopters from within the team who produce the best content. This type of content creation in a competitive setting could take considerable energy to manage.

The proposed implementation requires permission from players to establish their profile in the system and an undertaking from players to either create or participate in the creation of additional content for sponsor rewards. This would likely have to be negotiated and explicitly included in their official seasonal contracts. Note: next season's contracts have already been offered and signed for 2018, so were the proposal to be introduced it could not appear before 2019 season.

Crowd-source sponsors are required to own a virtual currency wallet in order to participate, setting one up and purchasing Ether at an exchange or through a crypto-wallet e.g. Mist. (Ether can be exchanged for Bitcoin and other cryptocurrencies via Shapeshifter, Kraken or other exchanges.) While token-based video and mobile games are common in sports contexts, there is very little skill required to participate in the reward systems of those games. Here, the same level of upskilling is required simply to sponsor your favourite players as it takes to become a crypto-currency trader.

The Crypto-kittie network slowdown in early December 2017 is a worrying development for any business trying to conduct a service over Ethereum. Gas prices across the whole network doubled, causing many transactions to be lost (simply not included by miners in the transaction bundles that make up a block). Gemini a digital asset trading platform ceased all trading in Ether for a short period in order to protect user trades.

Conclusion: problem-solution 2
It is unlikely this system would be adopted by fans or by the Club.
For fans or potential crowd-source sponsors, the technical know-how required to set up virtual currency wallets, the fluctuating Gas price for transactions and the unpredictable value of their donations (Ether value fluctuation) are all factors against adoption.

For the Club, opting to build the system as a set of smart contracts on a public blockchain introduces risk and additional technical requirements. The lack of system control and additional costs (in the form of transaction costs) and a cumbersome value exchange path from utility token (if created) to Ether and back to fiat currency e.g. Euro, if value is to derive from the system, are major drawbacks.

Problem-solution 3 – Proof-of-origin verification service

This system was tested on a permissioned Multichain blockchain (selected in comparative analysis in Chapter 2) with 2 AWS server nodes: one public, read-only accessible to the web interface and one admin server to initiate the root chain and write information to the blockchain using Multichain's Streams transaction feature.
A single publicly accessible, read-only access blockchain was initiated on which to verify the proof-of-origin of Bohemian FC assets to customers at point-of-sale.

Method: Impact assessment (Multi-Level output: 4.1)
These results are summarised in Table 5.28 on p. 92.

Method: Force-field analysis

Force-field analyses are investigations of forces that drive or restrain the implementation of new or re-engineered processes.

In this instance, there is some up-skilling for a marketing admin person to create the content and the body of the transaction that is subsequently queried by customers via QR pointer to the web-app.

Customers using the facility must be mobile-tech savvy and have / or download a QR reader on their mobile phone. These are easily found free-of-charge on mobile App and Play stores.

Impact assessments: **Outcomes of Test Phase: Problem-solution 3**

Topic	**Description**	**Time**	**Quality**	**Support**	**Comment**
Set-up	2 AWS servers Apache2 Ubuntu 16.4 Multichain 2.0 preference installations unique PKI Certificates	1 days	resilient, redundant, secure.	Wide community support for all set-ups	A fair degree of technical know-how required to set up servers and install all dependencies: some personalising and tweaking defaults required. Public server access can be scaled if query requests scale.
Implement	tweak the design and implement the permission system, asset structure and distribution model	2 days	Robust though inflexible - arising from immutability.	How-to do things is clearly sign-posted in Multichain FAQ	Visibility of transactions and the ability to point to where the data is using the Streams publishing feature is attractive. Maximum file size is 2MB. Some file compression advised.
Consensus	Proof-of-work with a low difficulty setting for private chain. Little energy wasted. No transaction fees.	ongoing -across mining nodes	Excellent	FAQ	Consensus is achieved almost instantly and block confirmation occurs within a 15 second timeframe.
Usability	CLI interface and Multichain Explorer GUI Bespoke interfaces for admin and end users	1-2 hours to learn	Accessible	Commands available on Multichain website and in Help command. FAQ required for bespoke interface.	The CLI interface is simple to use and easy to understand for a technical person. The Explorer GUI is functional and simple to use. A bespoke interface created for both admin and end user to simplify and declutter the interface.
Security	PKI SSH to servers / nodes. One admin role to oversee server / multi chain install.	ongoing	System is simple and robust. Some small training required.	Requires oversight. Identified as being that of Admin Node.	Mistakes are easily made regardless of technical ability: no roll-back feature. Mistaken entries will not be accessible for user queries.

Table 5.28 Outcomes of Test Phase for Problem-Solution 3: proof-of-origin web service

Conclusion: problem-solution 3

It is possible this proposal will be adopted by the Club. Unlike the two previous proposals, it doesn’t require negotiating cross-Sectional co-operation or advanced technical up-skilling before it is implemented.

It is cheap to deploy and only requires a single delegated person to create and publish content before it is publicly available.

The benefits to customers derive from awareness that consumer trust is an issue for them, this aligns with the core brand value of the Club as a community: ‘The People’s Club’.

Tackling brand piracy is of relevance in the wider sports and leisurewear marketplace and the gesture is welcomed by merchandise manufacturers Hummel and Club sponsors Mr Green.

In marketing terms the proposal offers an incremental improvement to the external perception of the quality of the goods on offer.

This use-case is selected for prototype demonstration purposes of this research. A bespoke interface was created for both admin and end user to simplify the interface. This was implemented according to the specification and written in php, javascript and html.

5.1.2 Multi-level design

Multi-level design is one of a number of techniques identified in the BPR success framework. It takes a semi-structured approach to forging a pathway between AS-IS system models to TO-BE process.

The technique requires progressively lower-level specification outputs at each of four stages throughout this process. In this orchestrated approach, the multi-level design requires outputs that would inform decision-making processes throughout the research.

Specification outputs:

1. risk assessment for introducing a blockchain-enabled system at Bohemian FC
2. problem-solution design pairings, blockchain feasibility study and QSOS evaluation

3. UML and architecture diagrams
4. impact assessment and force-field analyses

Level one output informed the high-level conclusion that blockchain technologies are indeed suitable for a distributed context such as that at Bohemian FC.

Level two output includes nine problem-solution design pairings arrived at through a decentralised consultation and innovation process, where end-user perspectives are given equal weight to those of daily involved process actors. The blockchain feasibility guidelines inform the selection of which problem-solution pairings to implement.

Level three output includes combined UML use case and architecture diagrams for three novel use cases for new systems processes at Bohemian FC. These specify what happens in each system and how.

Level four output is the evaluation of implementations, which inform the conclusion that one implementation is most-likely to be deployed given the context.

The multi-level design technique, deployed in this planned way assists decision-making throughout the orchestration design process. It successfully drives the process from AS-IS system models to TO-BE use-cases. It proved to be an effective means to identify candidate use cases that appropriately utilise the enhanced security and trust features afforded by the permanency or immutability of blockchain and other peer-to-peer technologies.

5.1.3 BPR success framework

Throughout the orchestration process this modified framework was deployed in a fluid and recursive fashion, offering a set of procedural guidelines and a body of examples from which to identify and add tools.

The BPR success framework offers a structured approach to information and insight gathering both at the Input and Output stages. This clear division between phases ensures that consideration is given to all aspects of a process in situ and the factors that will impact any new process adoption in the future.

The framework is useful on three fronts. Firstly, providing a checklist of key procedural elements to bear in mind. Secondly, providing a framework within which to document the discovery and implementation phases of this research. Thirdly, it contains within it, multiple example methods and techniques, some of which proved useful throughout the research process.

Description of methods and tools used throughout this research:	
Method / Tool	**Insight**
BPM risk assessment	High level perspective. References 6 core BPM capabilities.
Capability maturity assessment	A useful approach to determining where across stages of maturity a process or service (or organisation) is placed. These phases move from ad hoc to fully optimised.
Creative-thinking techniques	Visioning, PMI, out-of-the-box thinking. Unstructured techniques to envision new process systems. Suggested in PBR success framework.
Problem-solution design pairing	Distributed Digital Innovation approach to open innovation
Blockchain feasibility study	Identifies 6 useful implementation requirements for a blockchain system. 4 of 6 required to make a blockchain solution a viable one.
UML	Unified modelling language, a common standard used in software engineering to develop a system.
Impact assessment	Loosely defined approach to assessing impact of a new process. Suggested in PBR success framework.
Force-field analysis	Loosely defined approach to describing external factors which affect the implementation of a new process. Suggested in PBR success framework.
Multi-level design	Described fully above in the evaluation section. Suggested in PBR success framework.

Table 5.29 Assessment of methods and tools used throughout this research

The BPR success framework was used consistently throughout this research and is considered a key part of the successful and abundant identification of potential use cases.

5.2 Discussion

5.2.1 Blockchain technology

The aim of this research was to model an innovation methodology that would generate real-world use-cases that appropriately utilise the enhanced security and trust features (permanency and immutability) of blockchain and other peer-to-peer technologies. The research has successfully achieved this aim.

In doing so, a number of current issues for blockchain are further revealed, in particular the ongoing issues arising from immaturity. How immaturity affects the deployment of use-cases in the wild is touched on in the evaluation section 5.1 above, in particular in the Force field analysis of Ethereum public blockchain in use-case 2:
"The Crypto-kittie network slowdown in early December 2017 is a worrying development for any business trying to conduct a service over Ethereum. Gas prices across the whole network doubled, causing many transactions to be lost (simply not included by miners in the transaction bundles that make up a block). Gemini, a digital asset trading platform ceased all trading in Ether for a short period in order to protect user trades."

The blockchain community is divided on many issues, one of which is exemplified in the debate about private, permissioned vs public blockchains. In the impact assessments from the implementation models the benefits and weaknesses of each are described in context specific detail.

Arising from this research, the immaturity of public systems suggests that private, permissioned blockchains are more likely to be adopted in production contexts, for the foreseeable future.

Beyond cryptocurrency, one future for blockchain lies within the realm of data solutions, where different data management solutions are used collaboratively in a sort of polyglot persistence.

In 2006, Neal Ford introduced the term polyglot programming (Memeagora, 2016). He raised the idea that applications must maximise the opportunity inherent to multi-language environments in technology: namely that on the one hand, each language has strengths and weaknesses and on the other complex applications are host to complex problems.

Just as we can choose the right tool for a job, we can pick the right language for a given problem. Blockchain has a potential role in the polyglot overview of data management approaches.

5.2.2 The role of cryptography

Cryptography is a fundamental feature that underpins blockchain technology. Cryptography serves two functions in a blockchain. The first is to obscure private data in a public forum: the distributed public data-store or ledger. The second is to validate block order and achieve consensus among nodes.

In the prototype implementation cryptography is used both in the blockchain consensus model and in the Javascript front-end to obscure the details posted to the stream. Firstly, data published to a Multichain stream must be in binary-hexadecimal format. The input field data is converted from ASCII to base64 to binary-hexadecimal format. Additionally, in order to create and obscure data a Javascript crypto library is deployed to generate a Sha256 hash of the data field content is converted to bin-hex and used as a unique key to the transaction.

A comparison of permissioned vs. public blockchains could be conducted comparing transaction size, number of transactions, transaction sending delay, algorithmic specific parameters. However, in this research while these parameters are available for the private Multichain blockchain, they are not available for the public Ethereum chain as the implementation was deployed on the test net. The test net is not said to reflect the consensus time of the core.

On the private blockchain consensus is achieved almost instantly and block confirmation occurs within a 15 second timeframe.

5.3 Areas for Future Study

Areas for future study are identified as threat-modelling blockchain systems, an in-depth evaluation of front-end encryption requirements in publicly accessible blockchain systems and lastly, repeating the proof-of-concept orchestration model and generalising it to different contexts, technologies and environments. These are further detailed in Chapter 6.

5.4 Conclusion

This Chapter evaluates the orchestration model and reveals the strengths and weaknesses of the approach.

Blockchain technology is considered from a maturity perspective, private permissioned and public blockchains are discussed and the role of cryptography in implementation is examined.

Three areas for future study are identified.

6 CONCLUSION

6.1 Research Overview

The literature review began with an overview of distributed systems including decentralised autonomous organisations (DAO), the internet and the aspiring Inter-Planetary File System (IPFS). Distributed datastores were introduced including: blockchain, Hashgraph and Google Bigtable, a traditional distributed key : value distributed datastore.

The blockchain was identified as an example of a DAO and a force for disruption by disintermediation. Blockchain was described as a public record of verified, timestamped transactions maintained in an append-only, chain-like data structure. Distribution and cryptographic consensus models underpin the key features of permanency and immutability. Blockchain technology was explored from multiple perspective including: vulnerability, maturity and resilience.

A number of state-of-the-art innovation frameworks were explored: Capability Maturity Modelling, Business Process Redesign, Open Innovation and Distributed Digital Innovation, with a view to discovering useful approaches to inform a research strategy. Lastly the context under review, Bohemian Football Club was described.

An original two phase orchestration model was defined in Chapter 3. The model includes both a discovery and implementation phase. The key driving technique is multi-level design and the selected documentation framework followed a modified BPR success model identified by Vanwersch et al, (2016).

The implementation of the two-phase orchestration model was described in Chapter 4 and the process was documented according to six key procedural elements identified in the BPR success framework: aim, activity, actors, input, output and technique.

The results and outcomes were evaluated in Chapter 5. A single use case was selected as the most likely to succeed, given the impact assessment and force-field analysis results: proof-of-origin smart tagging solution.

Figure 6.11 Smart tagging solution overview slide. Source: F. Delaney

The orchestration model, multi-level design and documentation framework were also evaluated in Chapter 5.

Blockchain technology was analysed and discussed from a maturity perspective. The role of private permissioned and public blockchains were discussed and the role of cryptography in the implementation was examined.

6.2 Problem Definition

Blockchain technology is a relatively new research field and a number of gaps were identified: empirical research into network utility and blockchain performance metrics (number of transactions per second, block size, block confirmation), scoping potential business uses cases outside of the current primary cryptocurrency use case and usability from both end-user and developer perspectives.

This research focused on how best to identify, scope and develop software artefacts that utilise blockchain technology, such that the technology's potential is maximised and the real-world use case is enhanced.

The scope was limited to discovering and implementing blockchain-enabled use cases in a given context in the wild. Any use case that might successfully utilise blockchain technology was to be considered. Cryptocurrency valuation and trading were out of scope in this proof-of-concept research.

6.3 Design/Experimentation, Evaluation & Results

The research strategy relied on inductive reasoning and a mixed-method approach. The aim was to develop at least one use case where blockchain technology could enhance a business process in a given context in the wild: Bohemian FC - professional League of Ireland football club.

In order to identify and test potential blockchain use-cases in the wild an open innovation strategy was adopted. Akin to the ideation phase of an industrial design process, a two-phase orchestration model was designed in order to reveal as many potential use-cases as possible for deployment in the real-world setting. This phased orchestration model offers a qualitative, iterative, distributed modelling process informed by state-of-the-art innovation frameworks.

Phase one Discovery: scopes the existing context in order to discover potential candidate processes for redesign. These candidate processes while specific to one context can be repeated and generalised to further real world contexts.

Phase two Implementation: follows a traditional software development lifecycle and evaluation.

Given the amount of data generated during the process, the decision about how to document the research was important: a BPR success framework derived from a systematic literature review meta-model of successful process re-engineering projects was adopted - Vanwersch et al, 2016. Core headings include: Aim, Activity, Actors, Inputs (e.g. design catalysts), Outputs (e.g. AS-IS process models), Technique (e.g. Semi-structured - Multi-level design). It was deployed in a fluid and recursive fashion, offering a set of procedural guidelines and a body of examples from which to identify and add tools.

An evaluation of the orchestration model revealed the strengths and weaknesses of the approach these centre on its flexibility and soft boundaries. The orchestration model and multi-level design technique aimed to create one or more software artefacts arising from the implementation of the two-phase orchestration model. The results of the process include the four outputs of the multi-level design technique and three blockchain-enabled applications that were developed and tested.

The model succeeds in its aim to reveal as many potential use-cases as possible for deployment in a real-world context: identifying nine problem-solution design pairings, from which three met the feasibility criteria for blockchain enabled systems. This is considered to be an abundant outcome and suggests there is a lack of digital innovation approaches to devising blockchain use cases currently.

The weaknesses in the model stem from its strength: flexibility and fluid boundaries. A keen understanding of the goals of the frameworks involved and the purpose of the techniques and methods involved is required.

The approach is found to have successfully guided the research towards identifying a set of implementable blockchain-enabled systems at Bohemian FC. The proof-of-concept scoping strategy was deemed a success.

6.4 Contributions and impact

The design of an original two phase orchestration model has been defined. The model includes both a discovery and implementation phase and implements state-of-the-art process innovation frameworks: Capability Maturity Modelling, Business Process Redesign, Open Innovation and Distributed Digital Innovation.

The key guide is a multi-level design technique which drives the discovery phase from AS-IS system overview towards a new TO-BE system model.

The recommended documentation framework builds on a success meta-model of business process redesign projects identified by Vanwersch et al, (2016).

The aim of this research was to model an innovation methodology that would generate real-world use-cases that utilise the enhanced trust features of blockchain. The research has successfully achieved this aim.

The contribution is to have defined an innovation model through which context-specific blockchain use-cases can be identified and scoped in the wild.

6.5 Future Work & recommendations

Further study in this field may include threat-modelling for blockchain systems. The researcher found little research, during the course of this study period, threat-modelling would encompass a risk analysis that includes system immaturity.

Careful consideration of the purpose and specific requirements of front-end cryptography for blockchain-enabled systems would make an interesting future study field. How and why the publicly visible transaction timeline is required for a system will influence the degree to which the transaction details need to be obscured.

Additionally, the failure rate of encryption algorithms is increasing and keeping up to date with this aspect is important study.

The success of the orchestration model deployed here offers a promising future for identifying blockchain-enabled use cases in the wild. As a proof-of-concept methodology the approach has been proven successful. It would be interesting to see the process repeated and generalised to a different context to ascertain that the outcomes are equally successful.

BIBLIOGRAPHY

ACM Computing Classification System. (2012). Retrieved 3 January 2018, from https://www.acm.org/publications/class-2012

Baird, L. (2016). The Swirlds Hashgraph consensus algorithm: fair, fast, Byzantine fault tolerance (Whitepaper). Swirlds.

Baran, P. (1964). On distributed communications networks. IEEE transactions on Communications Systems, 12(1), 1-9.

Benet, J. (2014). IPFS: The Interplanetary Filesystem.

Berners Lee, T. (1989). The original proposal of the WWW. Retrieved 3 January 2018, from https://www.w3.org/History/1989/proposal.html

Bigi, G., Bracciali, A., Meacci, G., & Tuosto, E. (2015). Validation of Decentralised Smart Contracts Through Game Theory and Formal Methods. In Programming Languages with Applications to Biology and Security (pp. 142-161). Springer International Publishing.

Bitcoin - Open source P2P money. (2009). Retrieved 3 January 2018, from https://bitcoin.org/en/

Bohemian FC | Official club website. (2017). Retrieved 3 January 2018, from http://bohemianfc.com/

Buchman, E. (2016). Tendermint: Byzantine Fault Tolerance in the Age of Blockchains. University of Guelph, Cananda.

Buterin, V. (2014). A next generation smart contract and decentralized application platform. (Whitepaper) (p. 36). Ethereum.

Cameron, K. S., & Quinn, R. E. (2005). Diagnosing and changing organizational culture: Based on the competing values framework. John Wiley & Sons.

Chang, F., Dean, J., Ghemawat, S., Hsieh, W. C., Wallach, D. A., Burrows, M., ... & Gruber, R. E. (2008). Bigtable: A distributed storage system for structured data. ACM Transactions on Computer Systems (TOCS), 26(2), 4.

Chesbrough, H. (2012). Open Innovation: Where We've Been and Where We're Going. Research-Technology Management, 55(4), 20–27. https://doi.org/10.5437/08956308X5504085

Coindesk (2016). Lucas Abegg: Code is Law? Not quite yet.

Coindesk (2017) Gideon Greenspan: Where have all the private blockchains gone? Retrieved from https://www.coindesk.com/private-blockchains-gone/

Corda: Frictionless Commerce. (2017) Retrieved 3 January 2018, from https://www.corda.net/

DAO. (2015). The DAO Refunds - The Ethereum Wiki. Retrieved 3 January 2018, from https://theethereum.wiki/w/index.php/The_DAO_Refunds

Epicenter. (2017). EB107 – Gideon Greenspan: The Blockchain Is A New Database Paradigm. Retrieved from https://www.youtube.com/watch?v=T7F-kvackBQ

Ethereum Project. (2017). Retrieved 3 January 2018, from https://www.ethereum.org/

EU General Data Protection Regulation Foundation (GDPR) Training Course with Certification. (2017). Retrieved 3 January 2018, from http://eugdpr.institute/2018/jan/fas/about.html

Europol – EUIPO 2017 Situation Report on Counterfeiting and Piracy in the EU | Europol. (2017). Retrieved 3 January 2018, from https://www.europol.europa.eu/newsroom/news/europol-%E2%80%93-euipo-2017-situation-report-counterfeiting-and-piracy-in-eu

Gartner Hype Cycle for Emerging Technologies - Smarter With Gartner. (2017). Retrieved 3 January 2018, from https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

Ghemawat, S., Gobioff, H., & Leung, S. T. (2003, October). The Google file system. In ACM SIGOPS operating systems review (Vol. 37, No. 5, pp. 29-43). ACM.

Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. Financial Innovation, 2(1), 24.

Hammer, M., Champy, J., & Le Seac'h, M. (1993). Le reengineering (Vol. 26). Paris: Dunod.

Hardin, G. (1976). The tragedy of the commons.

Haughton et al. (2016). Blockchain: An Overview and Comparative Evaluation. CeADAR, Dublin.

Herbsleb, J., Zubrow, D., Goldenson, D., Hayes, W., & Paulk, M. (1997). Software quality and the capability maturity model. Communications of the ACM, 40(6), 30-40.

hummel® | Browse sportwear at hummel.net. (2017). Retrieved 3 January 2018, from https://hummel.net/

Internet Security Threat Report 2017 | Symantec. (2017). Retrieved 3 January 2018, from https://www.symantec.com/security-center/threat-report

Khan, R., & Hasan, R. (2016). The Story of Naive Alice: Behavioral Analysis of Susceptible Internet Users (pp. 390–395). IEEE. https://doi.org/10.1109/COMPSAC.2016.206

Kwon, J. (2014). Tendermint: Consensus without mining. Draft v. 0.6.

Lakshman, A. & Malik, P. (2010). Cassandra: a decentralized structured storage system. SIGOPS Oper. Syst. Rev. 44(2), 35-40. DOI=http://dx.doi.org/10.1145/1773912.1773922

Li, X., et al., (2017), A survey on the security of blockchain systems, Future Generation Computer Systems. Elsevier. DOI=http://dx.doi.org/10.1016/j.future.2017.08.020.

Mendling, J., Weber, I., van der Aalst, W., Brocke, J. vom, Cabanillas, C., Daniel, F., … Zhu, L. (2017). Blockchains for Business Process Management - Challenges and Opportunities. arXiv:1704.03610 [Cs]. Retrieved from http://arxiv.org/abs/1704.03610

Montelongo Arana, M. & Wittek, R.P. M. (2016) Community resilience: sustained cooperation and space usage in collective housing, Building Research & Information,44:7, 764-774, DOI: 10.1080/09613218.2016.1212514

Moore, T., Clayton, R., & Anderson, R. (2009). The Economics of Online Crime (Vol. 23). https://doi.org/10.1257/jep.23.3.3

MultiChain | Open source blockchain platform. (2014). Retrieved 3 January 2018, from https://www.multichain.com/

Nakamoto, S. B. (2008) Bitcoin: A peer-to-peer electronic cash system. http://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html

Nambisan, S., Lyytinen, K., Majchrzak, A., & Song, M. (2017). DIGITAL INNOVATION MANAGEMENT: REINVENTING INNOVATION MANAGEMENT RESEARCH IN A DIGITAL WORLD. MIS Quarterly, 41(1).

nealford.com • Polyglot Programming. (2006). Retrieved 3 January 2018, from http://nealford.com/memeagora/2006/12/05/Polyglot_Programming.html

Norta, A. (2015, August). Creation of smart-contracting collaborations for decentralized autonomous organizations. In International Conference on Business Informatics Research (pp. 3-17). Springer, Cham.

Cisco NetAcad. (2017). Retrieved 3 January 2018, from https://www.netacad.com/?utm_source=cdc&utm_medium=web&utm_campaign=netacad

Nylén, D., & Holmström, J. (2015). Digital innovation strategy: A framework for diagnosing and improving digital product and service innovation. Business Horizons, 58(1), 57–67. https://doi.org/10.1016/j.bushor.2014.09.001

O'Dwyer, K.J. et al. (2014). Bitcoin Mining and its Energy Footprint. 25th IET Irish Signals & Systems Conference 2014 China-Ireland International Conference on Information and Communities Technologies (ISSC 2014/CIICT 2014)

Rosemann, M., & vom Brocke, J. (2015). The Six Core Elements of Business Process Management. In J. vom Brocke & M. Rosemann (Eds.), Handbook on Business Process Management 1: Introduction, Methods, and Information Systems (pp. 105–122). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-45100-3_5

Schelling, T. C. (20). The strategy of conflict: [with a new preface] (Nachdr. d. Ausg. 1980). Cambridge, Mass.: Harvard Univ. Press.

Securities and Exchange Commission. (2017). Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO.

Sharma, S. (2015). An Extended Classification and Comparison of NoSQL Big Data Models. ArXiv:1509.08035 [Cs]. Retrieved from http://arxiv.org/abs/1509.08035

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. First Monday, 2(9). https://doi.org/10.5210/fm.v2i9.548

Tendermint Blockchain Consensus. (2016). Retrieved 3 January 2018, from https://tendermint.com/

United States Department Of Justice. Office Of Justice Programs. Bureau Of Justice Statistics. (2014). National Crime Victimization Survey: Identity Theft Supplement, 2012. ICPSR - Interuniversity Consortium for Political and Social Research. https://doi.org/10.3886/ICPSR34735.v1

Vanwersch, R. J. B., Shahzad, K., Vanderfeesten, I., Vanhaecht, K., Grefen, P., Pintelon, L., … Reijers, H. A. (2016). A Critical Evaluation and Framework of Business Process Improvement Methods. Business & Information Systems Engineering, 58(1), 43–53. https://doi.org/10.1007/s12599-015-0417-x

VeChain. (2017). Retrieved 3 January 2018, from https://www.vechain.com/#/

Venkatesh, V. (2014). Technology acceptance model and the unified theory of acceptance and use of technology. Wiley Encyclopedia of Management.

Von Hippel, E., & von Krogh, G. (2015). Crossroads—Identifying viable "need–solution pairs": Problem solving without problem formulation. Organization Science, 27(1), 207-221.

Von Rosing, M., von Scheel, H., & Scheer, A.-W. (2015). The Complete Business Process Handbook Extended Business Process Management. (Vol. 1). Morgan Kaufmann Pub.

W3C. (2017). Retrieved 3 January 2018, from https://www.w3.org/Consortium/

Wang, H., Chen, K., & Xu, D. (2016). A maturity model for blockchain adoption. Financial Innovation, 2(1). https://doi.org/10.1186/s40854-016-0031-z

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 151.

Wright, A., & Primavera, D. F. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia (SSRN Scholarly Paper No. ID 2580664). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2580664

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology? A Systematic Review. PloS one, 11(10), e0163477.

Zen, A. (2017). CryptoKitties | Collect and breed digital cats! Retrieved 3 January 2018, from https://www.cryptokitties.co

APPENDIX A

Field research summary

A summary of field research is given. Firstly, a summary of key points raised in interviews with management, staff, fans and professionals in sports retail external to the Club, followed by researcher observations of the context.

Interviews

Interviews with Club management / merchandising officers, fans and professionals in sports retail the following key point are derived:

The Club is keen to maintain, if not exceed existing levels of customer satisfaction amongst core fans and customer-base. There is a further, more abstract aim to enhance the sense of community beyond the Club into the wider community. Archival records and folk memory are important aspects of the culture of the Club, as is the strong visual identity cultivated in the Clubs social-media presence, printed material, graffiti and murals in the laneways around the grounds.

Abstractions such as authenticity, loyalty, quality and community are strong brand associations for the Club. There is also a visible nostalgia for past triumphs and various memorable occasions, football and otherwise at Dalymount Park and further afield when Bohemians played memorable away games. Nostalgia is particularly strong now that the Club will be renovated and must move from Dalymount Park while refurbishment is underway.

Core fans describe themselves as fans for life, and there are frequently generations of Bohs supporters in the same family. It seems that fans will buy at least one item of merchandise per season often buying considerably more.

Observations:

The sale of merchandise to the public represents a significant vertical in Club income (between 70,000 and 80,000 euro per annum). The process is overseen by a Club Officer and managed by two long-standing volunteers who understand their core customer-base intimately. They have considerable influence in stock and supply management and exhibit taste and foresight in their merchandise selections.

Cash-flow is an issue at different times of the year and it would appear that the merchandise income is a revenue buffer, subsidising other expenditure, which leads to poorer than optimal supplier relations and shorter credit lines than might be expected.
The system is not optimised for growth, rather it is constrained by limited sales resources, prioritising stock security over availability and a preferential servicing of on-premises sales over online sales.

APPENDIX B

Code excerpts from proof-of-origin prototype

Code extract from routes.php shows how data is published to a Multichain stream. Full code available to view on Github at: https://github.com/fgdel/vigilant-contractor

A signature or key is created from four data field inputs: name, email, message and small file (max size 2MB). These are encoded into a json array, converted to base64 and then converted to binary-hexadecimal to facilitate being written to Multichain.

Multichain confirms the transaction by returning an array with the transaction id, a url which is used to recover the transaction at a later date (via QR reader on mobile app) and a full set of the transaction details using the command getwallettransaction.

Blockhash, blocktime, url, signature, transaction id, number of block confirmations and a timestamp. The data field inputs are also available as: name, email, message and a the small file (max size 2MB) can be retrieved.

```
        $dataArray = array("signature" => $signature,"name" => $name,
"email"=> $email, "message"=>$message, "file"=>$dataFile);
        $dataJSON = json_encode($dataArray);
        $dataBase64 = base64_encode($dataJSON );
        $dataHex = bin2hex($dataBase64);

        //$info = $client->setDebug(true)->getInfo();
        $dataToReturn = array();
        $tx_id = $client->setDebug(true)->executeApi('publish',
array("public", $signature, $dataHex));

        $longUrl = $_SERVER['HTTP_HOST']."/details/".$signature;
        //$shorUrl = shortUrl($longUrl);

        $block_info = $client->setDebug(true)-
>executeApi('getwallettransaction', array($tx_id));
        $confirmations = $block_info['confirmations'];
        if($confirmations == 0){
            $blockhash = "NA";
            $blocktime = "NA";
        }
```

```
        else{
            $blockhash = $block_info['blockhash'];
            $blocktime = $block_info['blocktime'];
        }

        $dataToReturn['long_url'] = "http://".$longUrl;
        //$dataToReturn['short_url'] = $shorUrl;
        $dataToReturn['signature'] = $signature;
        $dataToReturn['transaction_id'] = $tx_id;
        $dataToReturn['confirmations'] = $confirmations;
        $dataToReturn['blockhash'] = $blockhash;
        $dataToReturn['blocktime'] = $blocktime;
        $dataToReturn['name'] = $name;
        $dataToReturn['email'] = $email;
        $dataToReturn['message'] = $message;
        $dataToReturn['timestamp'] = date('g:i A \o\n l jS F Y
\(\T\i\m\e\z\o\n\e \U\T\C\)', time());;

        return $response->withJson($dataToReturn)->withHeader('Content-Type',
'application/json');
        //return $response;
    });
```

APPENDIX C

Multichain set up and CLI command notes

Useful Multichain set up, CLI commands and Explorer install.

2-Node Demo

Set up Nodes (examples: not real)

Node Bohemians: ssh -i ……. ubuntu@00.00.00.00 <private 00.00.00.00>

Node B_Public: ssh -i ……. ubuntu@00.00.00.00 <private 00.00.00.00>

Addresses (examples: not real)

Node Bohemians: priv_chain1 ur2UDuhuT1Kks8MfJno8Efxd1AwMxKF2GSiM73

Node Bohemians: pub_chain2 1R3u9mJ5Z9Dkm6U9evbuxcZk8p4mMZU855hqkb

Node B_Public: pub_chain2 ny2hoDZsSCZnMgqsSVBa1anWZMGD7rqhgVB9R4

Chains (examples: not real)

priv_chain1: Bohemians<172.00.00.00>

multichaind priv_chain1@172.00.00.00:3333

rpcuser=multichainrpc

rpcpassword= QX3CTqSPeFURnCrcVtoS4opwj8DSVpKxJnYwc5uDQ

default-network-port = 7333 # Default TCP/IP port for peer-to-peer connection with other nodes.

default-rpc-port = 7334 # Default TCP/IP port for incoming JSON-RPC API requests.

pub_chain2: Bohemians<172.00.00.00>

multichaind pub_chain2@172.00.00.00:4444 <to connect to Bohemians node>

rpcuser=multichainrpc

rpcpassword=qYEfR6s2XsuwKwP77fr1pFTmqMx8LNhQuLvogS7yh

default-network-port = 4333 # Default TCP/IP port for peer-to-peer connection with other nodes.

default-rpc-port = 4334 # Default TCP/IP port for incoming JSON-RPC API requests.

pub_chain2: B_Public<172.00.00.00>
multichaind pub_chain2@172.00.00.00:4444 <to connect to B_Public node>
rpcuser=multichainrpc
rpcpassword=ohUiDeLk4NhCnfPQwnTnwq8AWsMRJPZNWR5jiej5X
default-network-port = 4333 # Default TCP/IP port for peer-to-peer connection with other nodes.
default-rpc-port = 4334 # Default TCP/IP port for incoming JSON-RPC API requests.

Create assets:
issue <address> <asset> 100 1
listassets

Create streams:
Node0:
create stream stream1 false #False means stream can only be written to by those with explicit
permission, to check: < list permissions stream1.*>
publish stream1 key1 73747265616d2064617461 #key : value pair, to check: <liststreams>
subscribe stream1
liststreams
listpermissions stream1.*
liststreamitems stream1
grant <address> receive,send #general send/receive perm for bc
grant <address> stream1.write #perm to write to specific stream

Node-n:
subscribe stream1
liststreamitems stream1
publish stream1 key1 736f6d65206f746865722064617461

publish stream1 key2 53747265616d732052756c6521

Query commands: #check API documentation for more

multichain-cli chain1 #access interactive mode on server

getblockchainparams

liststreamkeys stream1

liststreamkeyitems stream1 key1

liststreampublishers stream1 1VybW5DuvHhDtgjVabqxjFbtgrdJYkHjqbZTfu

liststreampublisheritems stream1

listassets <asset1>

getaddressbalances <1VybW5DuvHhDtgjVabqxjFbtgrdJYkHjqbZTfu>

gettotalbalances

getmultibalances

listwallettransactions

send <address> <asset name> <quantity>

or for multiples c/w data in hexadecimal format:

sendwithdata 1Ns4PgxxUAjdYBNfdQ9jw2ewcKnoB9ZgoZ2wED '{"kids_floodlight_7-8":1, "kids_floodlight_5-6":1}' 546865736520617265206f72206d792074776f206b69647320666f72206368726973746d61732e

useful…. (https://codebeautify.org/hex-string-converter)

getwallettransaction <txid of previous tx>

getwallettransaction 98e11f1b9e2fd41dd6a7e5dfa0ccf80c1a05482b233f22d4911e64d575e2fed8

Round Robin Mining:

Node1:

grant 1VybW5DuvHhDtgjVabqxjFbtgrdJYkHjqbZTfu mine #permission to mine <listpermissions mine>

Node2:

listpermissions mine

Multichain-explorer setup (examples: not real)

>>browser: 52.00.00.00:2222 #Node1 ip + port no.
exit interactive mode on Node1
Install dependencies for multichain-explorer (list on Github.com/multichain/multichainexplorer)

sudo apt-get install git
sudo git clone https:// <copy from github drop down>
ll #to list and check file is there
cd multichain-explorer
python setup.py install —user #recommended

————

cd ~/.multichain/chain1/
cat multichain.conf
grep rpc params.dat #copy rpcport=
echo “rpcport=4246” >> multichain.conf #use nano to edit mistakes!
cd #home
cd multichain-explorer
ll
cp chain1.example.conf chain1.conf #rename
sudo nano chain1.conf #to edit - using defaults here
python -m Mce.abe --config chain1.conf --commit-bytes 10000 --no-serve
#start
python -m Mce.abe --config chain1.conf #launches thread to listen on port <2750>, for tx every 60.0 secs

Ctrl + c in terminal window aborts thread.

Browser points to: 52.00.00.00:2750 #Node1 ip + port no. #config server Security group for port no.

Configure web demo:

sudo service apache2 status

ubuntu@….: ~/www/multichain-web-demo$ cat ~/.multichain/chain1/multichain.conf

rpcuser=multichainrpc
rpcpassword=BYWVXHq5jxVPtAhQ3k1oD JCZvo9xRKXzimBDAYhEiQB6
rpcport=4222

sudo cp config-example.txt config.txt
sudo nano config.txt

Note
[nohup multichaind <name> &] #to run in the background even if ssh terminates

[Node 1: ssh -i node-1-k.pem ubuntu@52.00.00.00
Daemon connect: multichaind chain1@172.00.00.00:4444
default-network-port = 4777   # Default TCP/IP port for peer-to-peer connection with other nodes.
default-rpc-port = 4778   # Default TCP/IP port for incoming JSON-RPC API requests.
Address Node1: sxpmNbqphp7W12LaiEfhKwhGzq7Csr2tMTU

Node 2: ssh -i node-1-k.pem ubuntu@34.00.00.00
Address Node2: btgrdJYkHjqbZTfu1VybW5DuvHhDtgjVab]