

Smart Contracts, Insurtechs and the Future of Insurance

Abtin Salahshor & John Scherrer

DIVISION OF INNOVATION ENGINEERING | DEPARTMENT OF DESIGN SCIENCES
FACULTY OF ENGINEERING LTH | LUND UNIVERSITY
2020

MASTER THESIS

hedvig



Smart Contracts, Insurtechs and the Future of Insurance

A study on digital technology adoption in a changing
competitive landscape

Abtin Salahshor & John Scherrer



LUND
UNIVERSITY

Smart Contracts, Insurtechs and the Future of Insurance

A study on digital technology adoption in a changing competitive landscape

Copyright © 2020 Abtin Salahshor & John Scherrer

Published by

Department of Design Sciences
Faculty of Engineering LTH, Lund University
P.O. Box 118, SE-221 00 Lund, Sweden

Subject: Innovation Engineering (INTM01)

Division: Innovation Engineering

Supervisor: Lars Bengtsson

Examiner: Jessica Lagerstedt Wadin

Abstract

The insurance industry is notoriously conservative and has seen comparably few technological improvements in the last fifty years. A wave of new technology-driven insurance firms, or insurtechs, is changing that. By leveraging new technology and offering more customer-centric and innovative products, these firms have captured shares in many insurance markets.

One technology — yet to be broadly adopted but with great hype — is blockchain-based smart contracts. These contracts promise to increase operational efficiency while simultaneously creating more equitable insurance products. Whether this is realistic is an entirely different matter; blockchain-based smart contracts have yet to prove tangible business value in insurance. Given the emergence of insurtechs and the growing interest in smart contracts, the purpose of this study is to increase knowledge of the strategic relevance and factors affecting adoption of smart contracts within the insurance industry — focusing on Swedish consumer-facing insurance applications.

The research is based on a triangulation methodology, consisting of a comprehensive literature review coupled with expert interviews concerning both smart contracts and the insurance industry. The study consists of a descriptive, exploratory and problem-solving component. The descriptive part-study resulted in a taxonomy of smart contracts; a strict (third-party-absent) and soft (third-party-present) definition. The exploratory part-study resulted in findings about the strengths and weaknesses of the technology; suggesting that soft smart contracts have a higher strategic fit than strict smart contracts in digitally mature and institutionally democratic markets. The problem-solving part-study — based on a case study of Swedish insurtech Hedvig — resulted in findings about realisable business value, particularly in claims management; suggesting that full automation is difficult for existing claims flows but possible for new insurance products. Finally, these empirical findings were combined with a set of conceptual frameworks to determine key drivers in the adoption of blockchain-based smart contracts and future scenarios.

Keywords: Smart contracts, Blockchain, Insurance, Insurtech, Diffusion theory, Adoption barriers

Sammanfattning

Försäkringsbranschen är ökänt konservativ och har sett relativt få teknologiska förbättringar under de senaste femtio åren. En våg av nya teknologidrivna försäkringsbolag, kallade *insurtechs*, håller på att förändra detta. Genom att utnyttja ny teknologi och erbjuda mer kundcentrerade och innovativa produkter, har dessa bolag fångat andelar av flera försäkringsmarknader.

En teknologi — som ännu inte spridits i stor skala men fått mycket uppmärksamhet — är blockkedjebaserade smarta kontrakt. Dessa kontrakt lovar att höja operationell effektivitet och samtidigt skapa mer rättvisa försäkringsprodukter. Huruvida detta är realistiskt är en annan fråga; blockkedjebaserade smarta kontrakt har fortfarande inte visat påtagligt affärsvärde inom försäkringsbranschen. Givet framväxten av *insurtechs* och det växande intresset för smarta kontrakt, är syftet med denna studie att öka kunskapen om smarta kontrakts strategiska relevans och spridningstakt inom försäkringsbranschen — med fokus på svenska konsumentmötande försäkringsapplikationer.

Studien baseras på en trianguleringsmetodik, i form av en omfattande litteraturstudie och expertintervjuer från domänerna smarta kontrakt och försäkringsindustrin. Studien består av en deskriptiv, explorativ och problemlösande del. Den deskriptiva delen av studien resulterade i en taxonomi för smarta kontrakt; en strikt (tredjepartsberoende) och simpel (tredjepartsberoende) definition. Den explorativa delen av studien resulterade i insikter om styrkor och svagheter hos smarta kontrakt, vilket indikerar att enkla smarta kontrakt har högre strategisk relevans än strikta i digitalt mogna och institutionellt demokratiska marknader. Den problemlösande delen (baserad på en fallstudie av svenska Hedvig) resulterade i insikter om realiserbart affärsvärde, framförallt inom skadereglering, vilket indikerar att komplett automation är svåruppnåeligt för existerande skaderegleringsflöden, men att nya försäkringar kan skapas genom smarta kontrakt. Slutligen applicerades empirin på konceptuella ramverk för att identifiera centrala diffusionsfaktorer för blockkedjebaserade smarta kontrakt samt framtida scenarion.

Nyckelord: Smarta kontrakt, Blockkedjor, Försäkring, Diffusionsteori, Adoptionsbarriärer

Preface

This master thesis examines the intersection of two subjects — the insurance industry and smart contracts — which are briefly introduced in Chapter 1. Within the insurance industry, the thesis has a particular focus on insurtechs — a new type of technology-driven insurance firm. Smart contracts are coupled with the technology behind them, conventional or otherwise, and studied through the lens of the insurance industry. Smart contracts' relevance and urgency for insurance will be the issue of study in this thesis.

The thesis has been done in collaboration with Lund University's Faculty of Engineering and Hedvig. For the entirety of the project, the thesis authors have been located at the Hedvig headquarters in Stockholm.

We want to thank John Ardelius, CTO at Hedvig, for inviting us to conduct this thesis and providing guidance along the way. Likewise, we are grateful for and deeply appreciate the advice and support of our supervisor at the Faculty of Engineering, Lars Bengtsson.

Finally, we want to express gratitude towards the entire Hedvig staff. Thank you for welcoming us through your warm and inspiring culture – and engaging us to join in.

Lund, January 2020

Abtin Salahshor & John Scherrer

Table of contents

List of definitions	I
1 Introduction	1
1.1 Background	1
1.2 Purpose	2
1.3 Delimitations	3
1.4 Report Structure	4
2 Method	6
2.1 Research Strategy	6
2.2 Data Collection	8
2.3 Data Analysis	13
2.4 Research Ethics	14
2.5 Research Credibility	14
3 Insurance Industry	17
3.1 Insurance: How It Works	17
3.2 Value Chain	18
3.3 Ecosystem	19
4 Smart Contracts	27
4.1 Definition	27
4.2 Blockchain as a Platform	32
4.3 How Smart Contracts Work	36
5 Conceptual Framework	38
5.1 Diffusion Theory	38
5.2 Design Thinking	40
5.3 The Grid	40
6 Strengths and Weaknesses of Smart Contracts	42

6.1 Strengths	44
6.2 Weaknesses	50
6.3 The Strict Case	60
6.4 The Soft Case	63
7 Case Study: Hedvig Applications	65
7.1 What Have We Learned?	65
7.2 Existing Claims Flows	69
7.3 New Claims Flows	76
7.4 Pay-per-use Opportunities	79
8 Adoption Barriers	80
8.1 Epidemic Model	80
8.2 Probit Model	83
8.3 Density Dependence Model	86
8.4 Technology Variant Model	88
8.5 Factors Driving Diffusion	89
9 Future Scenarios	93
9.1 Scenario 1 — Minimal Blockchain Adoption	93
9.2 Scenario 2 — Widespread Blockchain Adoption	95
10 Conclusions	98
10.1 Answers to Research Questions	98
10.2 Respondent Validation	103
10.3 Transferability	104
10.4 Recommendations to the Case Organisation	105
10.5 Contribution to Theory	105
10.6 Critical Review	106
10.7 Suggestions for Further Research	107
10.8 Final Remarks	107
References	109
Appendix A Proof of Concept for Train Delay Smart Contract	116
Appendix B Interview Guides	120

B.1 For Smart Contract and Blockchain Experts — Round 1	120
B.2 For Smart Contract and Blockchain Experts — Round 2	120
B.3 For Insurance Industry Experts	121

List of definitions

<i>Term</i>	<i>Definition</i>
<i>Bitcoin</i>	A digital currency based on a peer-to-peer network and cryptographic tools (Xu et al., 2017).
<i>Block</i>	A block contains a list of transactions, a unique cryptographic hash code and a reference to the previous hash code (Christidis & Devetsikiotis, 2016).
<i>Blockchain</i>	A blockchain is a public ledger distributed over a network that records transactions executed among network participants (Gatteschi et al., 2018b).
<i>Consensus protocol</i>	A mechanism that allows clients within a blockchain network to protect and preserve information records that are complete, unaltered and verifiable records of all transactions that have been made (Hans et al., 2017; Wood, 2014).
<i>Cryptocurrency</i>	A digital asset that is constructed to function as a medium of exchange, premised on the technology of cryptography, to secure the transactional flow as well as to control the creation of additional units of the currency (Chohan, 2017).
<i>Cryptography</i>	A method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it (Pawliw & Richards, 2018).
<i>Distributed public ledger</i>	A distributed public ledger can be considered a decentralized database holding information records (Shrier et al., 2016).
<i>Ethereum</i>	The most popular platform for constructing blockchain-based smart contracts (Luu et al., 2016).

<i>Hash</i>	A mathematical function that maps a given set of data to a fixed-size sequence of symbols (Gatteschi et al., 2018b).
<i>Mining</i>	The process of adding new blocks to the blockchain data structure (Xu et al., 2017).
<i>Merkle root</i>	The hash of (one or several) transactions in a block (Wang et al., 2017).
<i>Node</i>	A computer connected to the blockchain network that stores a copy of the public ledger. Some nodes also mine to verify transactions (Krawiec et al., 2016).
<i>Oracle</i>	An interface between smart contracts and the outside world (Bartoletti & Pompianu, 2017).
<i>Permissioned blockchain</i>	A blockchain, in which transaction processing is performed by a predefined list of subjects with known identities (Garzik, 2015).
<i>Permissionless blockchain</i>	A blockchain, in which there are no restrictions on identities of transaction processors (i.e., users that are eligible to create blocks of transactions) (Garzik, 2015).
<i>Private blockchain</i>	A blockchain, in which direct access to blockchain data and submitting transactions is limited to a predefined list of entities (Garzik, 2015).
<i>Public blockchain</i>	A blockchain, in which there are no restrictions on reading blockchain data (which still may be encrypted) and submitting transactions for inclusion into the blockchain (Garzik, 2015).
<i>Peer-to-peer (P2P)</i>	Refers to the decentralised interactions between two parties or more in a highly interconnected network. Participants in a P2P network deal directly with each other through a single mediation point (Blockgeeks, 2017).
<i>Soft smart contract</i>	Computer programs intended to digitally facilitate, verify, or enforce the search, negotiation, commitment, performance or adjudication of a contract and which can automatically move digital assets according to arbitrary pre-specified rules (Salahshor & Scherrer, 2020).

<i>Strict smart contract</i>	Soft smart contracts that can also be consistently executed by a network of mutually distrusting nodes, without the arbitration of a trusted authority (Salahshor & Scherrer, 2020).
<i>Insurance claim</i>	A request to the insurer for either coverage or compensation for the loss or event that the policyholder is covered against (Investopedia, 2020).
<i>Insurtech</i>	A technology-driven company, often a startup, that take advantage of the changing technological rules and customer expectations in the insurance market (Braun & Schreiber, 2017).
<i>Premium</i>	The amount of money an individual or business pays for an insurance policy (Investopedia, 2019).
<i>Property and casualty insurance</i>	The Property portion of Property and Casualty (P&C) insurance refers to coverage for personal belongings and property in the event that they are damaged or stolen. The Casualty portion of P&C insurance refers to coverage for incidents in which you are legally liable for property damage or injury caused to another party (The Zebra, 2019).
<i>Proxy</i>	A figure that can be used to represent the value of something else in a calculation (Lexico, 2019).
<i>Reinsurance</i>	The practice where an insurer transfers a portion of their risk to other parties by some form of agreement to reduce the likelihood of paying a large obligation resulting from an insurance claim (Investopedia, 2019).
<i>Underwriting</i>	The process where the insurer systematically measures the risks of an individual experiencing adverse effects compared to the average insured party and assigns monetary amounts to these risks (Association of British Insurers, 2014).

1 Introduction

This chapter aims to introduce the topic of the master thesis by stating the relevant background information and the issue of study. Moreover, the research questions and delimitations are presented.

1.1 Background

In 2017, the American insurance technology firm Lemonade set a world record (Schreiber, 2017). In a matter of seconds — three to be exact — it reviewed an insurance claim, compared it to the claimant’s insurance policy, ran anti-fraud algorithms, and delivered the appropriate payout. Being the insurance industry — characterized by a conservative, bureaucratic and sometimes hostile approach to its customers — the story made headlines.

It certainly is a remarkable technical feat. Many of us have experienced going through a frustrating claims process, which often feels like salt in the wound. New technology and a customer-centric approach is an opportunity to change that — which Lemonade has acted on. But what if the payout could have been delivered even faster? Before the claimant ever initiated the claim. Maybe even before he or she was aware of the damages done.

This is one of the many promises of smart contracts. Determining how real those promises are will be one of the purposes of this thesis.

1.1.1 Insurance: Conservatives and Their Challengers

The insurance industry is notoriously conservative (Nam, 2018) and has seen little change since the 1950s (Outreville, 1998). But unsurprisingly, digitalisation has come to impact even insurance, albeit later than similar industries like banking. Within the ecosystem of financial technology, or fintech, a new branch of insurance technology firms, or insurtechs, are emerging. Insurtechs challenge the industry status quo in a familiar way: (1) by leveraging the most advanced technologies, (2) focusing on improving the customer experience, and (3) having an agile culture that uses advanced analytics for organisational decision-making (Ricciardi, 2018).

Customer centricity — especially an emphasis on convenient experiences — has led many insurtechs to focus efforts on user-facing links in the insurance value chain (Svetlana, 2016). It is also here that insurtechs have had some of their most recognised successes: start-ups such as American Lemonade and Oscar Health; Indian Acko General Insurance; Chinese Zhong An; Swedish BIMA and Hedvig. However, there is some friction between the market and new technologies. While digitalisation and automation often increases convenience, lowers costs and saves time, there is increasing resistance to some aspects of digital omni-presence. Amplified bias in algorithmic decision-making (O’Neil, 2016), lack of transparency, and breach of privacy (Bartlett, 2018) are some examples. This balance is examined throughout the thesis project.

1.1.2 Smart Contracts: The Dual Promise of Efficiency and Fairness

Among general-purpose technologies (GPTs) with great promise and hype, such as artificial intelligence (AI) and blockchain, there is still considerable uncertainty about their practical application. One concept built on blockchain with particular promise for insurance is smart contracts.

Smart contracts powered by a blockchain could provide customers and insurers with the means to manage claims in a transparent, responsive and irrefutable manner. Contracts and claims could be recorded onto a blockchain and validated by the network, ensuring only valid claims are paid. For example, the blockchain would reject multiple claims for one accident because the network would know that a claim had already been made. Smart contracts would also enforce the claims – for instance, triggering payments automatically when certain conditions are met (and validated). (Deloitte, 2016)

Given this description, smart contracts could both increase the efficiency of insurance processes and ensure their transparency, which could improve the fairness of terms and conditions. The successful implementation of this technology, however, relies on critically gauging its strengths and weaknesses and identifying appropriate areas of application.

1.2 Purpose

The purpose of this paper is to increase knowledge of the strategic relevance and adoption of smart contracts within the consumer-focused home and travel insurance industry. Two aspects are investigated and analysed. First, how smart contracts can create value for insurers. Second, what barriers might affect the adoption of smart contracts and its technology in the insurance industry.

This is done through the following:

1. An assessment of smart contracts' strengths and weaknesses.
2. A case study of potential smart contract applications in insurance, using design thinking principles. The case centers on Swedish insurtech Hedvig.
3. An analysis of key adoption barriers, using a combination of empirical findings and diffusion theory.
4. An analysis of future scenarios for smart contracts in insurance, using design thinking principles through a modification of the Grid model.

Prior to doing this, however, the technology and industry must be properly understood. Therefore, some time will be spent detailing the properties of smart contracts and the competitive dynamics of the insurance industry.

1.2.1 Research Questions

The research questions can be separated into two parts. The former, in turn, consists of four sub-questions to ease the process of answering it.

Table 1.1: The research questions of this study.

RQ 1.	What are smart contracts and how can they be applied to the consumer-facing operations of Swedish insurtechs?	Chapter 9
1.1	How can insurtechs be described and understood?	Chapter 3
1.2	How can smart contracts be described and understood?	Chapter 4
1.3	What strengths and weaknesses do smart contracts have and how does it manifest in the insurance industry?	Chapter 6
1.4	What possible and concrete smart contract applications exist for Swedish insurance firms?	Chapter 7
RQ 2.	What factors hinder adoption of blockchain-based smart contracts in the Swedish insurance market, and how can they be overcome?	Chapter 8

1.3 Delimitations

The insurance type in focus will be property and casualty (P&C), otherwise known as home and travel insurance. Blockchain technology will only be described in the context of smart contracts. The application areas in focus will be consumer-facing applications within insurance in general and claims management or pay-per-

use/micro-insurance in particular. The geographic areas of study will be broadly considered at first, then narrowed to only encompass the Swedish market. Moreover, Hedvig, a Swedish insurtech, will be the focal point of the case study.

1.4 Report Structure

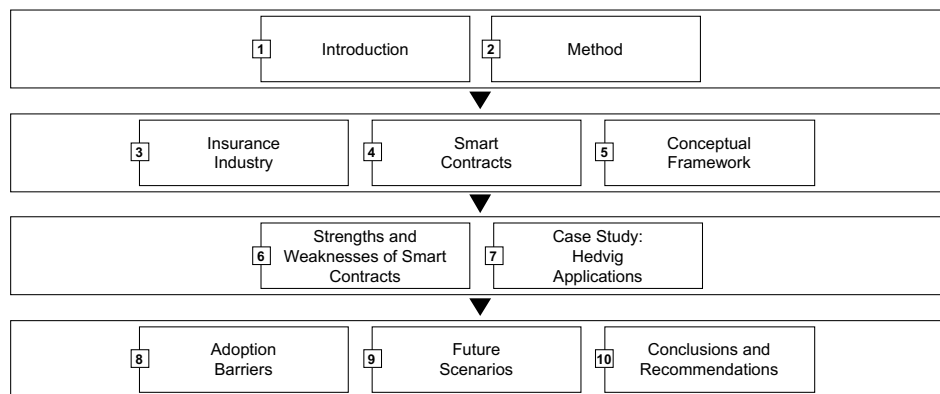


Figure 1.1: The chapters of the master thesis.

1.4.1 Chapter 2 – Method

A thorough description of the work process and method is presented. The chosen method is motivated through research strategy and project scope. Method validity, reliability, representativeness and objectivity is discussed.

1.4.2 Chapter 3 – Insurance Industry

A structural description of the insurance industry is presented. The competitive landscape is mapped with special emphasis on insurtechs as new entrants. The insurance value chain is presented, as is the Swedish insurance context.

1.4.3 Chapter 4 – Smart Contracts

A smart contract definition is discussed, and a taxonomy is developed. This is followed by a description of blockchain technology and its relevance for smart contracts. The importance of oracles as information channels is highlighted.

1.4.4 Chapter 5 – Conceptual Framework

A description of selected theories, concepts and models used in the later analysis is presented, which are mainly diffusion theory and design thinking principles. These are later used to conceptualise micro and macro adoption barriers as well as future scenarios.

1.4.5 Chapter 6 — Strengths and Weaknesses of Smart Contracts

A description of smart contracts technologies' strengths and weaknesses related to the insurance industry is presented, based on the definition taxonomy and blockchain design choices. A strength/weakness matrix is developed to synthesise the findings. Based on design thinking principles, a checklist is developed for determining the appropriateness of a smart contract solution for a specific claims flow.

1.4.6 Chapter 7 — Case Study: Applications in Hedvig

Hedvig is explored as a testbed for smart contract applications in insurance. This is done by looking at both existing insurance products and potentially new ones. Existing claims flows are assessed based on the above-mentioned checklist. A technical schematic is developed as a proof-of-concept (i.e. prototype) for a new insurance smart contract.

1.4.7 Chapter 8 — Adoption Barriers

Empirical data is synthesised. A comparison with diffusion theory aims to determine the explanatory force of different models. Factors that drive diffusion are presented.

1.4.8 Chapter 9 — Future Scenarios

A discussion on the future technology strategies of insurers based on different degrees of blockchain adoption is presented, using design thinking principles in a modified Grid model. This chapter uses the accumulated empirical findings to extrapolate trends.

1.4.9 Chapter 10 — Conclusions and Recommendations

The master thesis project's conclusions and recommendations are formulated. A summary of answers to the research questions is presented. Respondent validation is connected to the thesis results. Transferability is discussed. Recommendations to the case organisation and contributions to theory are presented. A critical review of the results is discussed. Finally, suggestions for further research are given.

2 Method

In this chapter, a thorough description of the work process and method is presented. The chosen method is motivated through research strategy and project scope. Method validity, reliability, representativeness and objectivity is discussed.

2.1 Research Strategy

A research strategy is an action plan created to achieve the goal of the research. It broadly outlines the logic and reasoning of the research and details actions that address the research goals (Denscombe, 2017). In this study, the goals consist of the purpose and research questions described in Section 1.2.

The research strategy was mapped after defining the purpose of the study, aligning the assignment with Hedvig's goals and deciding on the scope of the project. A high-level action plan of the work process is illustrated in Figure 1.2.

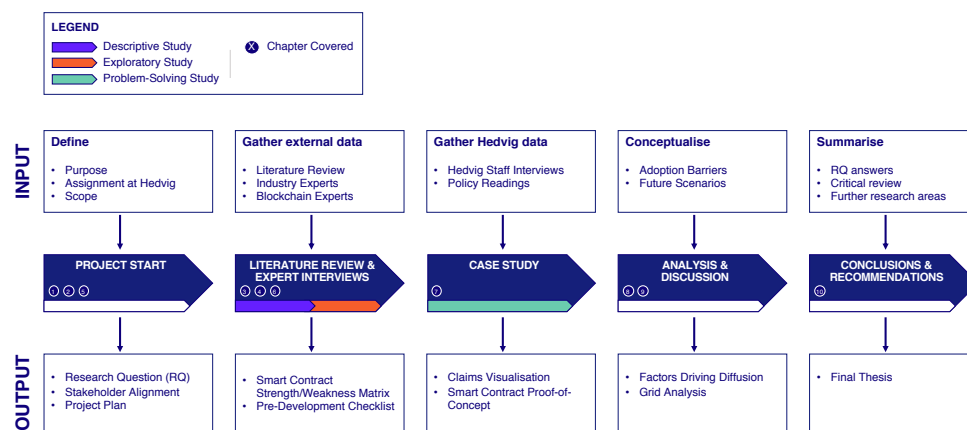


Figure 1.2: Master thesis work process.

Due to the varying characteristics of the research questions, the research strategy consists of a combination of studies, including a descriptive, exploratory and case

(problem-solving) part. The purpose of a descriptive study is to describe how a subject works (Höst et al., 2006). In this study, the descriptive part aims to give a fundamental understanding of what smart contracts and the insurance industry are and how they work. An exploratory study, on the other hand, aims to understand a subject in a deeper sense. The purpose of the exploratory part of this study is to give a thorough understanding of the strengths and weaknesses of smart contracts, how they apply to the insurance industry, and what factors might hinder or facilitate adoption within insurance. A problem-solving study aims to find a solution to an identified problem. In this study, the problem-solving part answers how a Swedish insurance company, in this case Hedvig, can apply smart contracts in their business, what benefits they might reap from it and what challenges have to be overcome for successful exploitation. A case study research approach was chosen to understand how the complex relationships between factors affect each other in a particular setting. The approach can provide deep knowledge on a specific subject but does not generalise conclusions to other cases (Höst et al., 2006). In the Hedvig case, conclusions are not generalised for other industries or geographies.

There are two main research strategy variants: qualitative and quantitative research. Qualitative research uses non-numerical data such as words or pictures as the unit of analysis and tends to have a contextual perspective on how multiple factors interrelate. Quantitative research uses numerical data as the unit of analysis and uses mathematics and statistical analysis to test hypotheses and study variables (Denscombe, 2017).

For the purposes of this thesis, a qualitative research approach was selected. This approach enables a flexible and iterative process for formulating research questions as well as collecting and analysing data (Denscombe, 2017). It allows for open-ended questions during expert interviews and yields a holistic perspective in the analysis.

2.1.1 Research Approach

The research approach follows an abductive logical reasoning, which is a combination of inductive and deductive reasoning. An inductive method is empirical and starts with observing cases, from which generalised rules can be derived. In contrast, a deductive method starts from a theory and hypothesised rule, which is tested by looking at its validity for one specific case (Timmermans & Tavory, 2012). This study seeks to do two things. First, to identify patterns and relationships in data to build new theories about a specific subject. Here, an inductive method was most useful for the research. Second, as these theories emerged from the research, they were applied and tested in the case study on Hedvig to investigate their validity and bring new insights from a relevant sample.

A research methodology can either be fixed or flexible. A study using a fixed methodology is defined before starting to execute the work. A flexible methodology

can be adjusted continuously due to changes in conditions that affect the study (Höst et al., 2006). Since the results from the early stages of the research might have steered the direction of the research in later stages, a flexible methodology was chosen. This enabled iterations on the scope and purpose of the study, adjusting them to be more relevant as new insights emerged through the work process.

2.2 Data Collection

The data collection consisted of two parts: external and internal data collection. The external data collection includes the literature review and interviews with industry and technology experts. The internal data collection included interviews with Hedvig staff.

2.2.1 Methods

Data triangulation is the use of contrasting sources of information in the data collection (Denscombe, 2017). To increase the validity of the data and results, this study used a triangulation approach with three sources of data: published research, industry experts, and technology experts. The experts who were interviewed were either practitioners or academics within the insurance and/or smart contract and blockchain domains. The published research was studied through a literature review.

2.2.2 Literature Review

A proper literature review gives perspective on what research has already been made within a subject area, which ensures that new research adds to existing knowledge rather than reinventing it. Furthermore, the literature review enables the reader to familiarise with the subject of study (Höst et al., 2006).

In this study, the literature review compiled a variety of relevant scientific research on smart contracts and its technologies as well as the insurance and insurtech fields. This contextualised the problem area, making the foundation on which interviews were based. The complete list of literature is shown in Table 2.1.

The sources used in the literature review were found through two search engines:

- LUBSearch: the search engine for academic articles, journals, PhD theses, and more, provided by Lund University.
- Google Scholar: the search engine for academic articles, journals, PhD theses, and more, provided by Google.

Table 2.1: List of papers used in the literature study.

<i>Term</i>	<i>Definition</i>
<i>Alharby & van Moorsel, 2017</i>	Blockchain-based Smart Contracts: A Systematic Mapping Study
<i>Bartoletti & Pompianu, 2017</i>	An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns
<i>Braun & Schreiber, 2017</i>	The Current InsurTech Landscape: Business Models and Disruptive Potential
<i>Buterin, 2014</i>	Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform
<i>Cuccuru, 2017</i>	Beyond Bitcoin: An Early Overview on Smart Contracts
<i>Eling & Lehmann, 2017</i>	The Impact of Digitalization on the Insurance Value Chain and the Insurability of Risks
<i>Fairfield, 2014</i>	Smart Contracts, Bitcoin Bots, and Consumer Protection
<i>Gatteschi et al., 2018a</i>	Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?
<i>Gatteschi et al., 2018b</i>	To Blockchain or Not to Blockchain: That Is the Question
<i>Halaburda, 2018</i>	Blockchain Revolution Without the Blockchain
<i>Hans et al., 2017</i>	Blockchain and Smart Contracts: Disruptive Technologies for the Insurance Market
<i>Junis et al., 2019</i>	A Revisit on Blockchain-based Smart Contract Technology

<i>Hu et al., 2019</i>	Blockchain-based Smart Contracts — Applications and Challenges
<i>Luu et al., 2016</i>	Making Smart Contracts Smarter
<i>McFall & Moor, 2018</i>	Who, or What, Is Insurtech Personalizing?: Persons, Prices, and the Historical Classification of Risk
<i>Nicoletti, 2017</i>	The Future of FinTech — Integrating Finance and Technology in Financial Services
<i>O'Hara, 2017</i>	Smart Contracts — Dumb Idea
<i>Nam, 2018</i>	How Much Are Insurance Consumers Willing to Pay for Blockchain and Smart Contracts? A Contingent Valuation Study
<i>Puertas et al., 2017</i>	The Next Wave of Fintech — Redefining Financial Services Through Technology
<i>Raikwar et al., 2018</i>	A Blockchain Framework for Insurance Processes
<i>Raskin, 2016</i>	The Law and Legality of Smart Contracts
<i>Savelyev, 2016</i>	Contract Law 2.0: Smart Contracts as the Beginning of the End of Classic Contract Law
<i>Sklaroff, 2018</i>	Smart Contracts and the Cost of Inflexibility
<i>Skog et al., 2016</i>	Chasing the Tale of the Unicorn — A Study of Sweden's Misty Meadows
<i>Svetlana, 2016</i>	Insurtech: Challenges and Development Perspectives

Szabo, 1997¹

Formalizing and Securing Relationships on Public Networks

Wang et al., 2018

An Overview of Smart Contract: Architecture, Applications, and Future Trends

The keywords used in the literature search were “Smart contract”, “Smart contracts strengths”, “Smart contracts weaknesses”, “Smart contracts risks”, “Smart contracts opportunities”, “Smart contract applications”, “Smart contracts in fintech”, “Smart contracts in insurtech”, “Blockchain strengths”, “Blockchain weaknesses”, “Blockchain applications in insurance”, “Blockchain applications in insurtech”, “Insurtech”, and “Technology in insurance”. To ensure relevant results, the academic papers used in the literature review are not older than 20 years and published by trustworthy institutions and authors.

In addition to the academic literature, non-peer-reviewed literature such as books, industry reports from consulting and research agencies as well as website sources were used for background information and other non-analytical purposes.

2.2.3 Interviews

Before conducting interviews, an interview guide was created. The interviews were recorded and subsequently transcribed in large rather than word for word. If the interviewee was unavailable for a call, questions were answered via email instead.

Interviews can be structured, unstructured or semi-structured. Unstructured interviews use interview guides, where questions are sorted by subject, and aim to explore the interviewee’s perspective on the qualities of a specific phenomenon. The unstructured interview is characterised by having open questions and need not have the same order of questions in each interview, instead changing depending on the specific interview’s focus or the interviewee’s subject matter expertise (Höst et al., 2006). Given this study’s qualitative research approach, an unstructured interview form was chosen as most suitable. The questions covered insurance industry practices, the insurtech trend as well as smart contract technology, its strengths and weaknesses, and potential uses within insurance.

The interviewees were chosen to represent a wide variety of people within the chosen industry and technology boundaries. Thus, the interview population includes

¹ The Nick Szabo article is an exception to the 20-year rule in the literature review, since it is considered foundational and pioneering within the field. A great deal of the literature refers to his articles in some way.

professors, researchers, entrepreneurs, consultants, business leaders, and more. Many of them have senior roles within their organisations and years of experience from relevant contexts. The complete list of interview subjects related to insurance and technology are shown in Table 2.2 and Table 2.3, respectively.

Table 2.2: List of experts within the insurance industry.

<i>Interviewee</i>	<i>Role</i>
<i>John Ardelius</i>	Co-Founder and Chief Technology Officer, Hedvig
<i>Ludvig Brisby Jeppsson</i>	Co-Founder, Incito
<i>Karl Jernberg</i>	Member Experience Specialist, Hedvig
<i>Pär Karlsson</i>	Senior Advisor, Insurance Sweden
<i>Thomas Nelander</i>	Head of Claims, Hedvig
<i>Anders Valentin</i>	Co-Founder and Chief Technology Officer, Undo

Table 2.3: List of experts within blockchain and smart contract technology.

<i>Interviewee</i>	<i>Role</i>
<i>Ian Arden</i>	Chief Executive Officer, Applicature
<i>Jake Brukman</i>	Co-Founder, CoinFund
<i>Martin Crillesen</i>	Business Developer, OpenLedger
<i>Alexander Fred-Ojala</i>	Chief Data Scientist, SCET Berkeley

<i>Hanna Halaburda</i>	Senior Economist, Bank of Canada
<i>Fritz Henglein</i>	Head of Research, Deon Digital
<i>Felix Kruuse</i>	Product Owner, Debricked
<i>Dmytro Lennyi</i>	Senior Delivery Manager, Intellias
<i>Juho Lindman</i>	Associate Professor, University of Gothenburg
<i>Sebastian Wain</i>	Co-Founder and Chief Executive Officer, CoinFabrik
<i>Gaspar Wosa</i>	Director of Automation and AI Innovation, Ericsson

The interviews were conducted in two rounds. The first round with industry experts focused on fundamentally understanding the Swedish insurance landscape and trends. The first round with technology experts focused on the fundamentals of smart contract technology, its definition in relation to blockchain technology, its potential application areas in insurance, and briefly its strengths and weaknesses. The results from the first round laid the knowledge base for creating the second interview guide. The second round with technology experts aimed to dive deeper into smart contracts' strengths and weaknesses as well as how they create business value within insurance.

2.3 Data Analysis

The process of a qualitative analysis can be divided into four main steps: data collection, coding, grouping, and conclusions (Höst et. al., 2006). A great deal of time was spent codifying the collected data (i.e. the reviewed literature and the full interview transcripts). This was done by marking important statements in the data and connecting them to one or several keywords, then structuring it in work documents. By grouping the coded text, patterns in opinions and reasoning about certain keywords or concepts were identified, either in certain subsets or the total sample. Based on these observed patterns, new theories were formed about the subject, which were subsequently applied in the case study to test their practical value. This part of the research followed the same four-step analysis process. Due

to the fact that the research was qualitative, using statistical models would not serve a purpose as in a quantitative study (Höst et. al., 2006). What was key was the occurrence of specific words and concepts.

Lastly, the empirical data was analysed using two conceptual frameworks: diffusion theory and design thinking. These frameworks were fitted to the data in order to contextualise the empirical findings, give new perspectives, and identify potential discrepancies between theory and practice. In Chapter 8, four diffusion models were compartmentalised into factors which could explain diffusion. These factors were then compared to the empirical findings and background data. Subsequently, factors driving diffusion could be identified. Similarly, in Chapter 9, future scenarios were developed by using design thinking through a modified Grid model to group and conclude smart contract technology strategies.

2.4 Research Ethics

Four key principles underlie the code of ethical research (Denscombe, 2017):

- Protecting the interest of the participants.
- Ensuring that participation is based on informed consent and is voluntary.
- Avoiding deception and operating with scientific integrity.
- Complying with the laws of the land.

Based on these principles, guidelines for managing ethical dilemmas and legal issues were considered. For this study, the highest risk factor was inappropriate use of confidential information obtained through conversations with firms in the insurance and crypto-technology industries. To mitigate this risk, the collected data has only been available to the thesis authors, and interviewees were offered to take part of transcribed interviews to ensure that their information was not misinterpreted, misrepresented, or confidential. The participants of the study were offered the option to remain anonymous before being interviewed and had to give consent to participate and getting recorded.

2.5 Research Credibility

2.5.1 Validity

Validity is the relation between the object of study and what is actually measured. It is essential that the measurements in a study align with the overall purpose of it. To increase the validity of a study, several methods for studying the same object can be used (Höst et al., 2006). In this study, the triangulation approach combined data

from multiple types of sources, with contrasting backgrounds within each type. For interviews, the guides were developed with special consideration for not directing or biasing the interviewee toward certain answers. Additionally, respondent validation (Denscombe, 2017) was used on the results and conclusions of the study.

2.5.2 Reliability

Reliability is how trustworthy the data collection and analysis are with respect to random variations (Höst et al., 2006). To achieve reliability, a study should give the same results if performed with the same research instrument by someone else (Denscombe, 2017). Due to the qualitative nature of the study, speaking with diverse interviewees and getting respondent validation were the primary ways of increasing reliability.

2.5.3 Generalisability

Generalisability can be understood through representativeness and transferability. The representativeness of a study is the degree of which results represent the whole population, which relies on the data source or sample (Höst et al., 2006). While case studies should not be generalised (Denscombe, 2017), the case study on Hedvig is focused on aspects of insurance that are quite industry generic. Thus, it is not unreasonable to discuss whether some of the case study findings can be generalised to a broader context. Transferability refers to the likelihood of the occurrence of some findings in another setting (Denscombe, 2017). The representativeness and transferability of this study are discussed in Section 10.3 and 10.6.

2.5.4 Objectivity

The objectivity of a study is to what degree the research can produce findings that are unbiased by the researcher (Denscombe, 2017). The main stakeholders in this study are the authors, Lund University's Faculty of Engineering, and the insurtech Hedvig. None of the authors have any financial incentives for doing this study, and there have been no conflicts of interest between Lund University and Hedvig. All stakeholders have stated interest in a factual review of the subject. Moreover, Hedvig has explicitly expressed a desire for the conclusions to be public in order to push the field forward.

In qualitative data collection, such as interviews, the interpretation of data can affect the results and thereby the objectivity of the study. Respondent validation mitigates the risk of having inaccurate information in the results. However, the conclusions that are translated from those results are still subjective and based on the authors' individual perspectives and potential biases. In general, the authors strived towards

objectivity by discussing interpretations of different situations openly — always seeking new perspectives and questioning their own.

Finally, when analysing the qualitative interviews, the authors have considered potential incentives that might exist for each interviewee. Entrepreneurs who are building products based on smart contracts might be inclined to speak positively about the technology compared to researchers that have less personal stake in its success. However, since the investigated subject in this study is a new technology, it is inappropriate to offhandedly disregard statements that do not refer to scientific research. A breadth of perspectives is highlighted in this study, and the goal is to give a nuanced view on the subject.

3 Insurance Industry

In this chapter, a structural description of the insurance industry is presented. The competitive landscape is mapped with special emphasis on insurtechs as new entrants. The insurance value chain is presented, as is the Swedish insurance context. This study focuses on property and casualty insurance (P&C), in which home and travel insurance are the most common policies. As previously mentioned, the study is limited to the consumer-facing parts of P&C insurance.

3.1 Insurance: How It Works

An insurance is a financial product in the form of a contract (i.e. insurance policy) that protects an individual against loss. The policyholder (i.e. insurance customer or user, claimant, or the insured) pays the insurer (i.e. insurance company) a premium, where the premium size is determined through an underwriting process. During underwriting, the insurer systematically measures the risks of an individual (i.e. measuring the policyholder's likelihood of experiencing adverse effects compared to the average insured party) and assigns monetary amounts to these risks (Association of British Insurers, 2014).

In case of a loss, a policyholder can file an insurance claim. A claim serves to protect the policyholder against a financial loss. The claim is a request to the insurer for either coverage or compensation for the loss or event that the policyholder is covered against. Once the claim is validated and approved by the insurer, they issue a payment to the policyholder or an approved party on behalf of the insured (Investopedia, 2019).

The insurance business model is based on policyholder premiums, which constitutes the revenue stream, and claims payouts coupled with the insurers' operating costs, which constitutes the main cost structure. The value creation comes from pooling premiums from policyholders with a variety of risk types and paying out money to the few policyholders that actually need to file insurance claims. Since it is unlikely that all policyholders in the pool will suffer from the events they are insured against, the liquidity requirements are dramatically reduced and the accumulated premiums sufficient (Tunstall et. al., 2018).

3.2 Value Chain

The insurance value chain can be broken down into seven primary activities based on Porter's value chain (Eling and Lehmann, 2018): marketing; product development; sales; underwriting; contract administration and customer service; claims management; and, asset and risk management. These are the activities needed to deliver an insurance product or service. The value chain is illustrated in Figure 3.1.

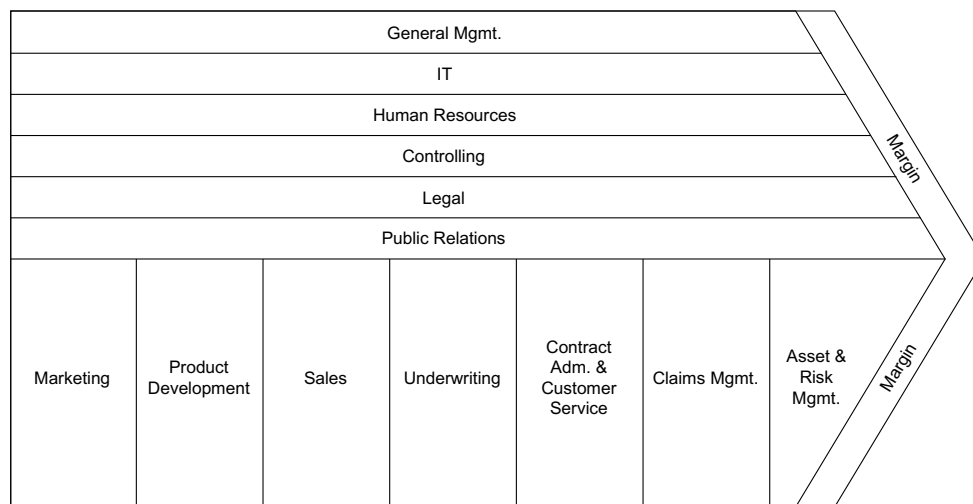


Figure 3.1: The insurance value chain. (Eling & Lehmann, 2018)

The tasks associated with each primary activity are described in Table 3.1.

Table 3.1: Tasks in the insurance value chain. (Eling & Lehmann, 2018).

<i>Primary Activity</i>	<i>Tasks</i>
Marketing	<p>Research ideas for product development.</p> <p>Analyse target groups.</p> <p>Develop pricing strategy.</p> <p>Design advertisements and communication strategy.</p>

<i>Product Development</i>	Build insurance products. Price products. Check legal requirements.
<i>Sales & Distribution</i>	Acquire customers. Sell products. Manage after-sales.
<i>Underwriting</i>	Handle applications. Assess risk. Assess the final contract details.
<i>Customer Administration & Service</i>	Change contract data. Answer customer requests.
<i>Claims Management</i>	Investigate fraud. Settle claims.
<i>Asset Management</i>	Allocate assets. Manage asset liability.
<i>Risk Management</i>	Analyse and manage risk.

3.3 Ecosystem

As of 2016, the insurance industry had roughly \$15 trillion in assets under management and \$5 trillion in annual premium revenues (Cusano, 2016). P&C insurance accounts for 30% of these premium revenues (McKinsey, 2019). Despite its size and appeal to investors, insurance has seen fewer technological improvements than other financial service sectors (Cusano, 2016). Furthermore, insurance is among the industries where customer satisfaction and loyalty ratings are the lowest (Dickinson, 2015).

But the insurance market is facing a transformation (Braun & Schreiber, 2017). New technologies combined with changing customer demands are advancing digitisation, which intensifies competition and enables faster offers, more personalised services, and more transparency. To meet the rising expectations in digital customer experiences, insurers are starting to digitalise their value chains. These advances are changing the playing field, from traditionally slow-moving to fast-paced and technology-driven.

3.3.1 Incumbents and the Insurance Tradition

There is a variety of traditional insurance company types. The insurance incumbents highlighted in this section are primary insurers and reinsurers.

A primary insurer, also known as a ceding company, can be described as an insurance company that first sells insurance to a client, and then purchases reinsurance (HarperCollins, 2019). If an insurance company writes policies to a large number of customers that are all subjects to a specific risk, an unusual but major event (e.g. a natural catastrophe) could accumulate enormous losses for the primary insurer. Also, some few individuals can encounter events that would imply claims of substantial amounts. To protect its net liability on individual risks, large or multiple losses, the primary insurer can partner with a reinsurance company. Reinsurance can be described as “insurance for insurance”. The reinsurance company takes a portion of the risk portfolio held by a primary insurer on agreed terms. By diversifying its risk portfolio, the primary insurer can reduce the probability of having major losses from insurance claims, and therefore underwrite more policies covering a higher quantity of risk (Investopedia, 2019). The reinsurer can generate profits from underwriting and insuring a portfolio with low risks of devastating claims costs, as well as by investing premiums and achieving returns on them (Caplinger, 2017).

During recent years, more traditional insurance and reinsurance companies are screening the insurtech landscape for opportunities in technology that can help them gain a competitive edge. This is a result from accelerated innovation efforts in the insurance industry, which has led to increased pressure on firm performance (Braun & Schreiber, 2017). Insurance incumbents could address this issue through partnerships, in-house technology development, incubation of technology startups, or a multi-sided strategy that includes several of these options (KPMG, 2015).

3.3.2 Entrants and the Technology Infusion

From the changing digital landscape and customer expectations, a new wave of companies has emerged in the insurance industry — often referred to as insurtechs. Insurtech is a field that has grown out of the fintech ecosystem, which can be

described as “initiatives, with an innovative and disruptive business model, which leverage on ICT in the area of financial services” (Nicoletti, 2017). Despite few technological improvements and low customer satisfaction in the insurance industry, the insurtech startup scene emerged late compared to the fintech companies applying new digital technologies to the banking and finance sector. During the past years, insurtechs have gained traction. Their growth of funding volume increased explosively from \$140 million in 2011 to \$1.7 billion in 2016 (Braun & Schreiber, 2017).

There is no agreed-upon definition of insurtech, but there are patterns in how insurtechs are described. Insurtechs are technology-driven companies, often startups, that take advantage of the changing technological rules and customer expectations in the insurance market (Braun and Schreiber, 2017). They drive innovation, act fast, disrupt traditional business models, and digitise along the whole insurance value chain. Insurtechs rapidly spot future customer needs and position themselves and their offerings accordingly.

Insurtechs stand out from incumbents in three important regards (Ricciardi, 2017):

1. They leverage the most advanced technologies.
2. They follow a user-centric approach to improve the customer experience.
3. They have an agile culture and leverage advanced analytics for decision-making.

Insurtechs are thus in a position to be first-movers in many new technologies, finding applications that incumbents might not have perceived due to lacking customer centricity. This creates a good foundation for insurtech-incumbent partnerships, which is often necessary since many insurtechs only occupy a subset of the insurance value chain and can only exist by offering a product in partnership with a larger insurance incumbent. In fact, some argue that insurtechs exist with the goal of creating value for both customers and insurance incumbents (Lewis, 2017).

Insurtechs often operate platforms where users purchase specialised contracts, which are held and underwritten by larger insurance companies who have the legal and financial infrastructure to create policies and carry risk. By partnering with larger insurance companies with strong cash positions, they can avoid regulatory barriers such as capitalisation requirements. Other insurtechs overcome such requirements through extensive venture funding or peer-to-peer (P2P) solutions, where clients are also investors and get returns in surplus premiums from their peer investors’ policies (Ricciardi, 2017).

Following a user-centric approach, insurtechs have improved the insurance customers’ purchase journey (Ricciardi, 2017). By simplifying both internal operational processes and consumer-facing parts of the value chain (e.g. claims management and underwriting), they increase customer centricity in an industry that lags in convenience and clarity.

Often, insurtechs are led by technology-driven entrepreneurs that are skilled at quickly developing, testing and bringing new solutions to the market. In comparison to traditional financial institutions, insurtechs have smaller and focused teams working in a more lean and agile way, with a mindset more prepared for learning through failures and performing fast iterations (Ricciardi, 2017).

There are, of course, insurtechs that operate in parts of the insurance value chain that do not relate to improving the end insurance customer experience. There is a mix of companies with varied offerings, business models and roles in the ecosystem. Insurtechs can be divided into nine categories based on what they offer in the insurance ecosystem (distribution, risk carrier or technology), as shown in Table 3.2 (Braun & Schreiber, 2017).

Table 3.2: Insurtech categories (Braun & Schreiber, 2017).

	<i>Insurtech Category</i>	<i>What They Offer</i>	<i>Role in Ecosystem</i>
1	<i>Comparison Portals</i>	Enable online comparisons between various insurance products and providers.	Distribution
2	<i>Digital Brokers</i>	Brokerage of insurance policies through web-based portals or mobile apps.	Distribution
3	<i>Insurance Cross Sellers</i>	Offer insurance as complements to products (typically at the point-of-sale or in an own app).	Distribution
4	<i>Peer-to-Peer Insurance</i>	Bring together private parties for mutual insurance coverage.	Distribution & Risk Carrier
5	<i>On-Demand Insurance</i>	Offer coverage for selected periods of time.	Distribution & Risk Carrier
6	<i>Digital Insurers</i>	Offer fully digital insurance solutions that are only accessible via online channels.	Risk Carrier
7	<i>Big Data Analytics & Insurance Software</i>	Provide software solutions.	Technology
8	<i>Internet of Things</i>	Internet of Things.	Technology
9	<i>Blockchain & Smart Contracts</i>	Create solutions for a tamper-proof distributed database system for transactions.	Technology

An overview of some of the most well-funded insurtech companies is given in Table 3.3.

Table 3.3: Some of the most well-funded insurtechs as of now (CrunchBase, 2019).

<i>Company Name</i>	<i>What They Offer</i>	<i>Total Funding</i>
<i>Oscar Health</i>	A patient-centered health insurance to a low price by leveraging data and mobile technology.	\$1400M
<i>Zhong An</i>	Customer-centric insurance, with digital capabilities that enable immediate claims settlements and instant communications.	\$800M
<i>Root Insurance</i>	An affordable car insurance made possible by tracking driving patterns and only selling insurance to safe drivers.	\$530M
<i>Lemonade</i>	A fast, affordable and hassle-free P&C insurance with high transparency, where surplus premiums gets donated to charity.	\$480M
<i>Acko General Insurance</i>	An affordable car insurance plus micro-insurances around other companies' services.	\$110M

Clearly, many of these larger insurtechs tap into the characteristics proposed by Ricciardi. Many insurtechs operate under several of the categories presented in Table 3.2. For example, while being a full-fledged digital insurer, Lemonade also incorporates artificial intelligence to power its operations, reducing bureaucracy and the need for brokers and paperwork (Braun & Schreiber, 2017). Another example is Zhong An, a fully digitised insurtech that has started investing in blockchain technology, by developing a blockchain-based open platform for insurance transactions. Whether these insurtechs are currently using or considering smart contracts is unclear.

A PwC (2016) study showed that 90% of insurers fear losing business to insurtechs. With innovative business models and strong technological capabilities, concerns are rising that insurtechs could jeopardise the existence of insurance incumbents (Braun & Schreiber, 2017). But for the time being, many insurtechs are focusing on distribution rather than risk carrying; only a portion satisfy the capabilities required to be full-fledged insurance operators (Lewis, 2017). This could in fact help incumbents, by creating opportunities for them to access new clients through partnerships with insurtechs focusing on the customer interface (Oliver Wyman, 2016).

However, by entering insurtech-incumbent partnerships, incumbents that previously held an oligarchic position in the industry have to confront a more complex profit dynamic. Incumbents can trade a share of their profits for improved underwriting and access to new customers through user-centric insurance products, while letting

insurtechs have all direct communication with their customers. Losing brand contact and recognition with the consumer could prove dangerous in the long-term.

3.3.3 The Swedish Context

The Swedish insurance landscape is dominated by a handful of large incumbents. In 2018, just four insurance companies (Länsförsäkringar, Folksam, IF and TryggHansa) accounted for about 80% of the non-life insurance premiums, as shown in Figure 3.2. This corresponds to roughly 67 billion SEK, or \$6,75 billion (Insurance Sweden, 2019). These four large incumbents act as full-fledged insurers that cover the whole insurance value chain. Compared to other countries, Swedish insurance incumbents have achieved a higher degree of digital capabilities (Karlsson, 2019).

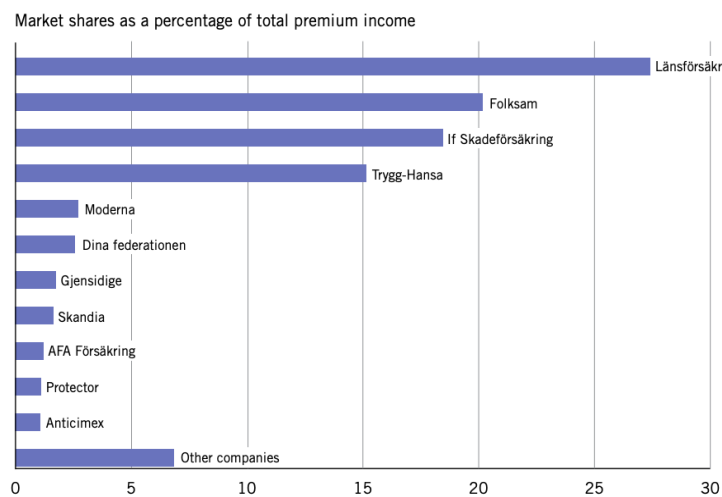


Figure 3.2: Swedish market shares for non-life insurance by firm (Insurance Sweden, 2019).

Puertas et al. (2017) breaks down the Swedish insurtechs into eight activity categories: underwriting and reinsurance; on-demand insurance; consumer communities (P2P); customer engagement; distribution; personalisation; risk detection and prevention; and, claims management and processing. For each category, they have identified Swedish companies that in a full sense or partly fall under the insurtech definition. The companies are illustrated in Figure 3.3.

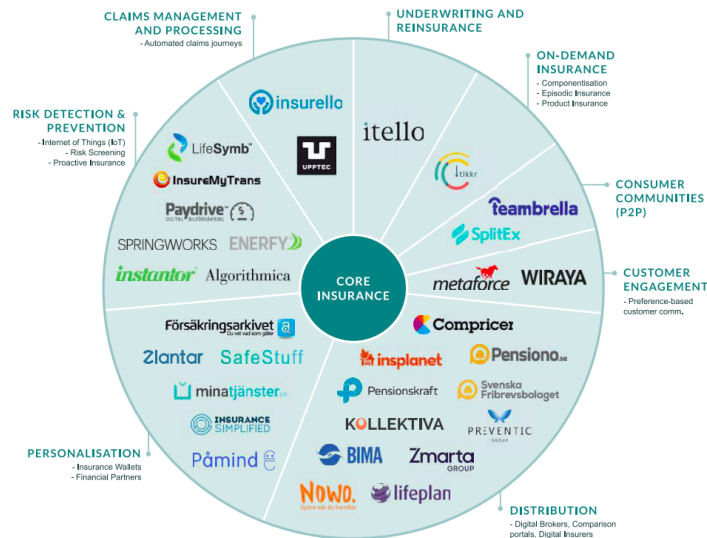


Figure 3.3: The Swedish insurtech landscape by activity (Puertas et al., 2017).

Although the insurtechs are gaining traction in Sweden in terms of funding volume, they still only make up a tiny fraction of global insurtech funding (Puertas et al., 2017). In 2016, Swedish insurtechs only accounted for 1% of the total insurance tech deals made globally (Statista, 2017). But funding is not the only factor that determines market potential. Swedish consumers are considered to be high-tech early adopters due to their high internet and computer literacy, and the country boasts a strong network of startups within the financial services sector (Skog et al., 2016). As such, the addressable market might be large relative to the population.

Pär Karlsson (2019), Senior Advisor at Insurance Sweden (the industry organisation for Swedish insurance), argues that the Swedish insurance incumbents do not see startup insurtechs as a threat, since the startups and incumbents do not necessarily compete for the same customers. Instead, he argues that there are synergies to be had: incumbents can gain access to new customer segments, and startups can benefit from incumbents' established infrastructure. Karlsson believes new ecosystems will emerge in which insurance companies specialise in narrower domains, and partner with companies with complementary abilities to a greater extent. Furthermore, the traditional insurance product portfolio might not look the same in the future (Karlsson, 2019):

I think that we are moving toward a development where insurers will offer insurance as a part of an offering consisting of different types of services. It could be various types of security services that aim to proactively minimise risks, rather than [just] providing coverage if the worst should happen. (Karlsson, 2019)

Puertas et al. (2017) suggest similar developments:

For incumbents, it is vital [...] to accommodate future insurance customers, who will demand proactive, personalised, and intuitive insurance products. Whereas incumbent insurers have already started to partner with startups in a selection of areas, they still face challenges in reinventing themselves for future policy holders. Further collaboration with Insurtech startups may prove a viable solution. (Puertas et al., 2017)

3.3.4 About Hedvig

This insurtech landscape is subject to rapid change, through which new companies emerge and others disappear (Puertas et al., 2017). Hedvig is an example of one of the emerging startups in the Swedish insurtech scene. Hedvig was founded in 2016 by Lucas Carlsén, Fredrik Fors and John Ardelius, driven by a need to change the governing dynamics of the insurance industry, which they argue disincentivise insurers from helping customers when they are in need (Carlsén, 2019).

The purpose of Hedvig is to provide a fairer and more user-centric insurance experience compared to incumbents. Their revenue model is based on taking a fixed fee from the insurance customers' premiums and pooling the rest for claims payouts. Should any surplus remain in the pool at the end of the year, it is given to charity. The flat fee enables Hedvig to act as an insurance company that is less incentivised to minimise the number of claims payouts. Furthermore, leveraging advanced technologies and using a digital-only interface towards customers has enabled them to simplify several steps in the traditional claims process, both for customers and internal operations. Hedvig acts as a risk carrier in the insurance value chain, selling their own insurance products, and is backed by reinsurer HDI (Carlsén, 2019).

Hedvig has raised around \$14 millions of venture funding and aims to go beyond its current product offering, which today consists of property insurance, and expand to countries beyond its home market (Lunden, 2019).

Hedvig's home insurance for apartments currently covers 15 000 customers and more than 10 billion SEK in property and contents (Hedvig, 2019). Today, their claims team — internally known as insurance experience (IEX) — consists of five full-time and four part-time employees. Being technology-driven, Hedvig is constantly looking for technical solutions to ease the burden of claims management and allow more focus on high-complexity cases. Automating routine tasks could not only serve that purpose, but also keep operational costs low when rapidly scaling the customer base. While the number of claims is likely to scale in linear proportion to the number of customers, the time spent on managing these need not follow the same pattern, if claims automation is consistently implemented. Thus, the value is twofold: attracting customers through quick and modern insurance experiences, and gradually relieving staff from routine tasks as the company scales (Ardelius, 2019).

4 Smart Contracts

In this chapter, a smart contract definition is discussed, and a taxonomy is developed. This is followed by a description of blockchain technology and its relevance for smart contracts. The importance of oracles as information channels is highlighted.

4.1 Definition

4.1.1 What Is a Contract?

To understand smart contracts, the fundamental concept of contracts must be understood. In his influential 1997 paper, the computer scientist and legal scholar Nick Szabo described a contract as “the main traditional way to formalize a business relationship” and a “set of promises agreed to in a ‘meeting of minds’” (Szabo, 1997). A contract can be both written and oral, although it is more often the former. A contract described in words (rather than code) is called a semantic contract.

There are five contractual phases (Szabo, 1997):

1. **Search:** Refers to anticipating, agreeing to, and clearly writing down the various eventualities that must be covered by a contract.
2. **Negotiation:** Refers to the simple haggling or more sophisticated exchange interactions between counterparts with regard to the terms of a contract, when there is a lack of common ground.
3. **Commitment:** Refers to the final agreement made between counterparts and their promise to honour a specified contract.
4. **Performance:** Refers to the execution of the terms of the contract.
5. **Adjudication:** Refers to the legal process of dispute resolution arising out of performance (or lack thereof).

Szabo (1997) saw in the future of our digital world a radical lowering of costs related to the areas of jurisdiction, trust and security, in the same way that technology had previously lowered costs in the areas of transportation, manufacturing and communication. When discussing smart contracts, Szabo (1997) had a particular focus on the performance stage, although all of them were to some extent described.

4.1.2 What Is a Smart Contract?

There is no clear-cut definition of the smart contract concept (O’Hara, 2017). This is troubling, considering how the definition profoundly impacts the discussion on business applicability and urgency. Therefore, some time must be spent on creating a taxonomy for smart contracts.

The earliest definition of smart contracts can be traced to Nick Szabo, who is consistently credited with being the concept pioneer (Hans et al., 2017; Wang et al., 2018; Bartoletti & Pompianu, 2017). In the broadest sense, Szabo (1997) defines smart contracts by stating that they “reduce mental and computational transaction costs imposed by either principals, third parties, or their tools”. He elaborates:

The contractual phases of search, negotiation, commitment, performance, and adjudication constitute the realm of smart contracts. [...] Smart contracts utilize protocols and user interfaces to facilitate all steps of the contracting process. This gives us new ways to formalize and secure digital relationships which are far more functional than their inanimate paper-based ancestors. (Szabo, 1997)

Szabo (1997) describes smart contracts as a secure and digital facilitator of the traditional paper-based contracting process. He emphasises lowering transaction costs, most notably at the performance phase of contracting (Szabo, 1997).

His definition pre-dated the concept of blockchain (see Section 4.3) by more than a decade (Nakamoto, 2008), which has since come to dominate the literature and is now almost an inseparable concept. During the second wave of blockchain technologies, described as Blockchain 2.0 and characterised by improved smart contract functionality, new blockchain-based distributed computing platforms were born, most notably Ethereum (Bartoletti & Pompianu., 2017; Gatteschi et al., 2018b).

In Ethereum’s white paper, smart contracts are described as “systems which automatically move digital assets according to arbitrary pre-specified rules” (Buterin, 2014). Where Szabo (1997) more broadly describes smart contracts as a digital system which lowers transaction costs, Buterin (2014) specifically highlights automation in contract execution — in other words, the idea of self-executing contracts. He also goes on to describe smart contracts as “cryptographic ‘boxes’ that contain value and only unlock if certain conditions are met” (Buterin, 2014). Again, the security aspect mentioned by Szabo (1997) appears, specifically worded in terms of cryptography or encryption.

What is interesting is how since the time of Szabo and Buterin, a vast majority of the literature has come to associate smart contracts directly with blockchain, almost having it as a prerequisite for a functioning smart contract. It is not entirely unexpected, since blockchain technologies and platforms such as Ethereum have been popularised and hyped both in business spheres and through public media, to which Halaburda (2018) draws parallels to the Internet at the time of the dot-com

boom. Some definition examples include that smart contracts are “full-fledged programs that run on blockchain” (Luu et al., 2016); “computer programs that can be consistently executed by a network of mutually distrusting nodes, without the arbitration of a trusted authority” (Bartoletti & Pompianu., 2017); “[supporting] automated interactions between the blockchain and existing transaction systems” (Raikwar et al., 2018); and “pieces of code stored on the blockchain that are programmed to behave in a given manner when certain conditions are met [and which] can be executed automatically without control of a third party” (Gatteschi et al., 2018b).

While some of these still explicitly mention automation there is a greater emphasis on the blockchain-based nature of the contracts. What this seems to imply is that for these authors, the defining attribute of a smart contract is the distributed or decentralised nature as well as the trustless or third-party-absent environment in which they could function. This functionality, while not synonymous with blockchain technologies, is today practically only possible at scale on the blockchain. This is hinted by Nam’s (2018) description:

*“Smart contracts **generally recorded onto a blockchain** and validated by the network are computer programs, the correct execution of which is automatically enforced by underlying legal agreement without relying on a trusted authority.” (Nam, 2018)*
[Bold font made by the authors of the thesis]

It is worth noting that while Szabo (1997) explores contract structures which allow the absence of a mutually trusted third-party, the third-party-absent characteristic of a smart contract was not intrinsic in the definition:

*Smart contracts **often involve trusted third parties**, exemplified by an **intermediary**, who is involved in the performance, and an **adjudicator**, who is invoked to resolve disputes arising out of performance (or lack thereof). Intermediaries can operate during search, negotiation, commitment, and/or performance. (Szabo, 1997)* *[Bold font made by the authors of the thesis]*

In fact, not all recent literature centers on blockchain, exemplified by the definitions that smart contracts are “computer protocols intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract” (Wang et al., 2018); “defined as agreements wherein execution is automated, usually by computers” (Raskin, 2016); and the “automated execution of transactions” (Halaburda, 2018). These all emphasise the self-executing nature of smart contracts rather than third-party-absence.

Others focus on other characteristics. Viewing smart contracts from a legal perspective, Raskin (2016) makes a distinction of strong and weak smart contracts based on the “costs of their revocation and modification”. If a court can with relative ease alter a contract after it has been executed, Raskin (2016) defines it as weak. This focuses on immutability or irreversibility, which is typical for the blockchain-based solution.

Some key characteristics of smart contracts can now be extracted from these definitions, as shown in Table 4.1 with their corresponding number of mentions in the literature review. The focus here is on explicit mentions, which of course disregards some implicit but essential characteristics such as smart contracts being digital, programmatic or secure. Also, the articles which explicitly mention blockchain-based as a characteristic may also implicitly suggest third-party-absence and decentralisation and vice versa.

Table 4.1: Smart contract characteristics explicitly mentioned in article definitions.

<i>Characteristic</i>	<i>Number of explicit mentions (out of 20)</i>
<i>Automated / Self-executing</i>	13
<i>Blockchain-based</i>	7
<i>Third-party-absent / Trustless</i>	6
<i>Decentralised / Uncensorable</i>	5
<i>Autonomous</i>	1
<i>Immutable / Permanent</i>	1

It becomes clear that two dimensions separate smart from regular contracts:

1. Automatic Enforcement vs Manual Enforcement
2. Absence of Third-Party vs Presence of Third-Party

The question that follows is whether a contract needs to be both self-executing and third-party-absent to qualify as smart. Arguably, no. While the self-executing, or digitally automated, nature of smart contracts has been inherent in its definition since Szabo's (1997) days, absence of third-party is something of a novelty. Moreover, a contract that is decentralised or trustless but non-digital is more akin to ancient community-based contracts than innovative smart ones, suggesting that third-party-absence is in and of itself not smart. This analysis allows for a strict and soft definition of smart contracts, as defined in Table 4.2 and Figure 4.1.

Table 4.2: The strict and soft definitions of smart contracts.

<i>Smart Contract Definition</i>	
<i>Soft smart contract</i>	Computer programs intended to digitally facilitate, verify, or enforce the search, negotiation, commitment, performance or adjudication of a contract and which can automatically move digital assets according to arbitrary pre-specified rules.
<i>Strict smart contract</i>	Soft smart contracts that can also be consistently executed by a network of mutually distrusting nodes, without the arbitration of a trusted authority.

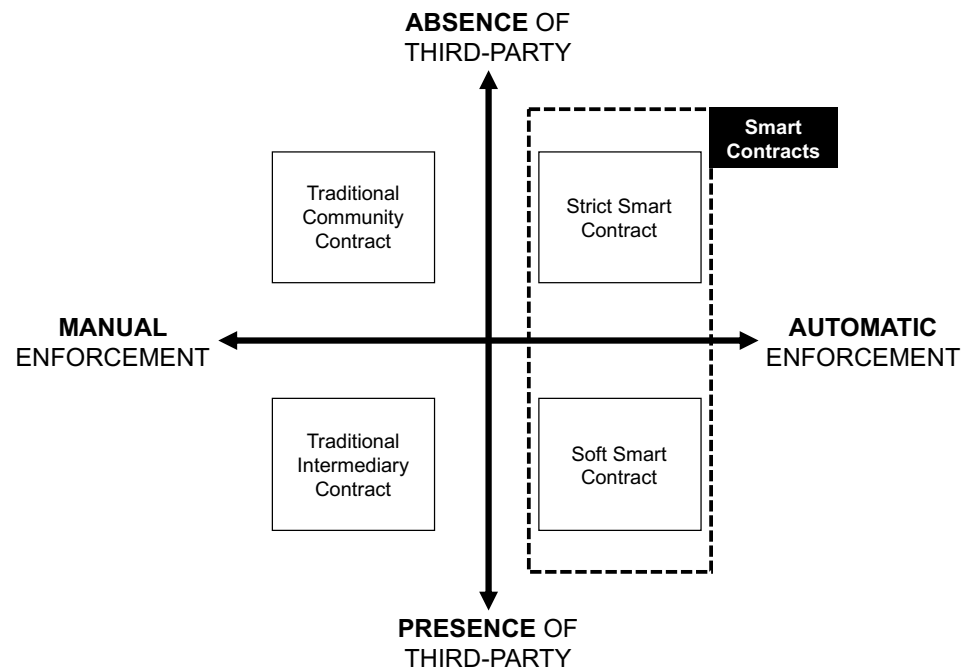


Figure 4.1: Taxonomy of smart contracts.

In this thesis, the emphasis will be on the contractual phases of negotiation and performance rather than search, commitment and adjudication.

4.2 Blockchain as a Platform

By now it should be clear that to satisfy the conditions of a soft smart contract, a blockchain solution is not necessary. However, it is still important to understand the fundamentals of blockchain technology for the purpose of strict smart contracts.

4.2.1 What Is a Blockchain?

A blockchain is a public ledger distributed over a network that records transactions executed among network participants (Gatteschi et al., 2018b). Some of these terms need further elaboration. A transaction refers to a message sent from one network node to another. A distributed public ledger can be considered a decentralised database holding information records (Shrier et al., 2016). In and of itself, this database is of little use since there is no structure that secures commonality (i.e. consistent information) across network nodes; that is, a system for everyone to agree on the record of transaction data. However, with the help of a consensus protocol (see Section 4.2.2), an environment is created that enables decentralised networks to trade without trust; that is, without needing a third-party authority. Thus, the blockchain incorporates complete, unaltered and verifiable records of all transactions that have been made (Wood, 2014), with consensus protocols being what allows clients within the network to protect and preserve those information records (Hans et al., 2017).

Blockchains can be thought of as a “DNA chain”, which grows longer over time as new information (i.e. transactions) is added to it. Transactions are time-boxed and grouped into blocks (hence the name “blockchain”) and sorted sequentially, so that each block is linked to the previous one. The chain is maintained by network participants, which verify transactions and add them to new blocks in a process called mining, which is an integral aspect of the consensus mechanism. (Gatteschi et al., 2018b)

Thus, blockchains are characterised by being distributed and immutable, which affords transparency and trust without reliance on powerful intermediaries. By replacing a mutually trusted third-party with a mutually trusted virtual computer (Szabo, 1997), blockchains offer more than just incremental technological improvements. To its most ideological supporters, it is a radical tool for power distribution away from big (often monopolistic) corporations or governments and into the hands of people (Sklaroff, 2018). This strain of anarchist or libertarian thought has been present especially in Bitcoin but is nonetheless an aspect to most blockchain platforms (Henglein, 2019).

Some blockchains have a native cryptocurrency: a digital asset that is constructed to function as a medium of exchange, premised on the technology of cryptography, to secure the transactional flow as well as to control the creation of additional units

of the currency (Chohan, 2017). On the Ethereum platform, which is the most popular platform for constructing strict smart contracts (Luu et al., 2016), the cryptocurrency is ether (ETH).

Blockchain technology in general, and its consensus protocols in particular, answer the question raised by Szabo in 1997: how does one formulate and secure relationships on public networks? This is also a reason why smart contracts have come to be so closely associated with blockchain technologies.

4.2.2 How Blockchains Work

There is an inherent problem in digital trade. Since there are no physical assets being exchanged, there is no natural law that prohibits a party from selling or gifting the same asset several times, even though the party no longer owns it. This is called the *double spending problem* and has two solutions (Junis et al., 2019). The first is a centralised approach in which a trusted third-party maintains the transaction record. The second is a decentralised approach in which a consensus protocol creates majority rule among networked nodes. The latter is the blockchain way.

To best explain how blockchain works, it is actually simpler to begin with the opposite (centralised) approach; that is, transactions with a mutually trusted third-party.

Let's say that one party, Alice, wants to transfer \$10 to another party, John. An intermediary (i.e. third-party) in this context would be a bank that facilitates the transfer. Once the bank received Alice's request, it can check if Alice has the funds necessary to complete the transaction. If she does, the bank will transfer the desired amount to John's account, simply by subtracting that amount from Alice's account and adding it to John's. This is possible because the bank alone administers and guarantees the integrity of the transaction records.

So, how would a consistent and untampered transaction record be secured without a mutually trusted third-party accounting for it? Let's say that Alice instead wants to transfer 10ETH (i.e. ether, the cryptocurrency of Ethereum) to John on the Ethereum blockchain. A good explanation for this is given by Gatteschi et al. (2018b) which is quoted for the remainder of this section in addition to being illustrated in Figure 4.3:

Cryptocurrency is stored in a digital wallet, which is identified by an address. To make the transfer, Alice specifies the desired amount to be transferred and the address of John's wallet. Then she broadcasts the transaction to the network. The transaction is digitally signed using secret information stored in the wallet, ensuring that it actually comes from Alice's wallet and that it cannot be altered by someone else.

In this case, the network consisting of other participants receives a decentrally broadcasted transaction request from Alice, rather than it being sent to a central authority, e.g. a bank.

Other network nodes check whether the transaction has been actually authorized by Alice by analyzing the digital signature. Then they verify if she is entitled to spend the money by computing her balance on a local copy of the blockchain (which stores all the transactions on the network, including transfers to and from her wallet). If the transfer can be made, the nodes insert the transaction in a new block.

Using private key cryptography, Alice's identity is validated by the network participants. Since each network participant has a local copy of the blockchain, they can then individually compute her balance to determine if she has enough assets to make to transfer. Once this is verified, the transaction is added to a block, which collects all the verified transactions during a specific timespan.

The new block contains a list of all the transactions to be validated, and records in its header a summary of them (the hash, a mathematical function that maps a given set of data to a fixed-size sequence of symbols) as well as of the previous block header.

At this point, the new block has still not been added to the blockchain. This means that until now, no consensus has been needed and is yet to be reached. This is when the mining process starts, which is the heart of a consensus protocol called *proof-of-work*.

To add the newly created block to the blockchain, nodes start the mining process—a competition in which the nodes have to solve a complex mathematical problem. This process, referred to as proof of work, requires nodes to find a random value that, combined with the hash of transactions and of the previous block header, produces a given result. When a node identifies a possible solution, it broadcasts the result to the other nodes, which check it. If the majority of the nodes agree on the result, the block is considered valid and it is added to the blockchain, making each node update its local copy (the winner could also receive a reward; for example, in the form of a transaction fee). As a result of the mining process, John will see that the amount sent by Alice has been received in his wallet.

To really understand how the connection between blocks is made, the contents of a block must be understood. This is shown in Figure 4.2. The hash of transactions in the new block is called a *merkle root*, which — together with (1) the hash of the previous block header, and (2) a random number — has to add up to a given result. This is a “puzzle” that has to be solved by the network participants. Since any change, however minor, in any transaction (TX) hash will change the entire merkle root, any manipulation of transaction data will be discovered when a claimed solution is broadcasted to the network. It will simply not add up to the given result of non-malicious network participants.

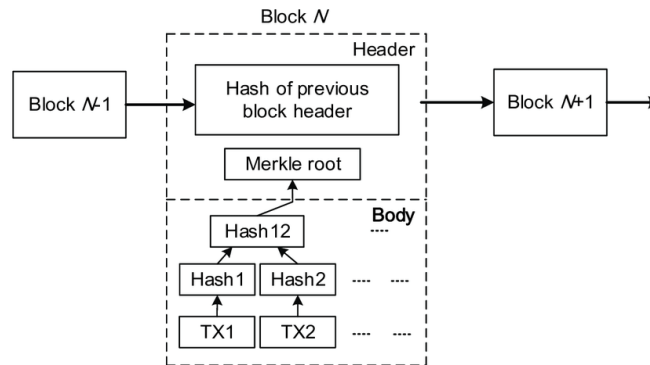


Figure 4.2: Blockchain structure (Wang et al., 2017).

Gatteschi et al. (2018b) continue:

Such a complex validation mechanism makes it nearly impossible for a node to control the majority of the network, as it would require extremely high computational power to create a false block, solve the mathematical problem before other nodes, and reach the 51 percent consensus on the just-mined block. Moreover, the fact that each validated block contains a reference to the previous block (secured using cryptography methods) prevents malicious modifications to recorded transactions. In fact, changing a transaction would also imply modifying the summary of the block containing it and of the blocks that follow. (Gatteschi et al., 2018b)

The link between block N and block N-1 through their hashes means that any manipulation at any point in the blockchain will be detected: the hashes will change, which requires changes along the entire chain, which requires enormous computational power.

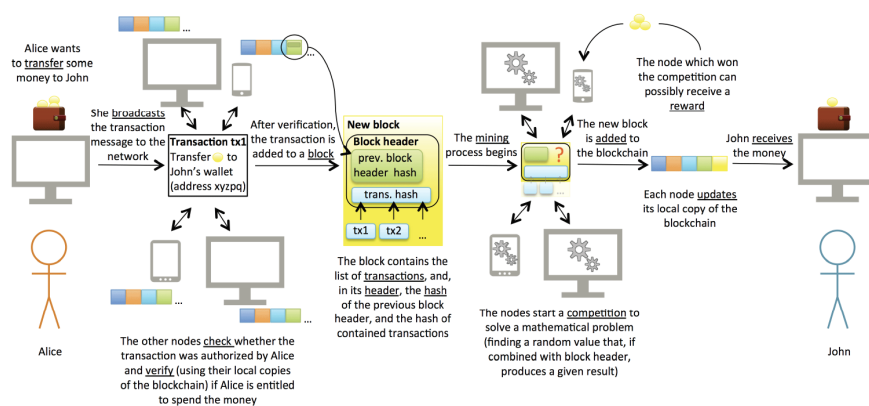


Figure 4.3: How blockchain transactions are recorded (Gatteschi et al., 2018b).

4.2.3 Visibility and Access

There are different degrees of visibility and access to particular blockchains. This is described in terms of two dimensions: (1) public or private blockchains (i.e. the right to participate in reading and submitting transactions) and (2) permissioned or permissionless blockchains (i.e. the right to participate in processing transactions) (Garzik, 2015):

1. **A public blockchain** is a blockchain, in which there are no restrictions on reading blockchain data (which still may be encrypted) and submitting transactions for inclusion into the blockchain.
2. **A private blockchain** is a blockchain, in which direct access to blockchain data and submitting transactions is limited to a predefined list of entities.
3. **A permissionless blockchain** is a blockchain, in which there are no restrictions on identities of transaction processors (i.e., users that are eligible to create blocks of transactions).
4. **A permissioned blockchain** is a blockchain, in which transaction processing is performed by a predefined list of subjects with known identities.

Garzik (2015) considers private, permissioned blockchain to be the least valuable; that is, those that least utilise the unique qualities of blockchain.

4.3 How Smart Contracts Work

4.3.1 The Soft Smart Contract

Since a soft smart contract is basically a digitally automated version of a classic contract, it can manifest in a variety of ways, many of which are today taken for granted or considered mundane. An example could be an automated recurring payment (i.e. direct debit) that someone sets up with a bank (Halaburda, 2018). There are some companies which leverage soft smart contract technology as a centerpiece of their business model (e.g. Earny and Woilá) and others still which use such technology as an add-on to their value proposition (e.g. AXA's Fizzy).

4.3.2 The Strict Smart Contract

Today, the execution of a strict smart contract is only feasible at scale by utilising blockchain technologies (Hu et al., 2019). The consumer-facing application of such smart contracts is less prevalent in existing business, but two examples are the companies Dynamis (Gatteschi et al., 2018a) and Etherisc (Bartoletti & Pompianu,

2017). Dynamis provides peer-to-peer (P2P) unemployment insurance (Foresight Factory, 2017), whereas Etherisc provides flight delay insurance and hurricane insurance, and is prototyping crypto-wallet insurance, crop insurance, and illness insurance, among other things (Etherisc, 2019).

4.3.3 Oracles as Information Channels

A smart contract consists of some essential building blocks. A study by Bartoletti & Pompianu (2017) attempts to quantify the “design patterns” of strict smart contracts built on Ethereum, which includes: (1) tokens, (2) authorisation, (3) oracles, (4) randomness, (5) polls, (6) time constraint, (7) termination, (8) math, and (9) fork check.

Some of the patterns are intuitive and need no further explanations. Others address challenges related specifically to blockchain technologies. Arguably, the most interesting pattern is *oracles*, which are used to acquire data from outside the blockchain. Since the Ethereum language does not allow contracts to query external sites (this would break the determinism of computations), oracles are used as an interface between strict smart contracts and the outside world (Bartoletti & Pompianu, 2017). This design pattern is only present in 7% of the smart contracts analysed by Bartoletti & Pompianu (2017), but is essential in consumer-facing insurance applications, which need to interact with both policyholder data and outside events that affect the policyholder.

5 Conceptual Framework

In this chapter, a description of selected theories, concepts and models used in the later analysis is presented, which are mainly diffusion theory and design thinking principles. These are later used to conceptualise micro and macro adoption barriers as well as future scenarios.

5.1 Diffusion Theory

The main piece of theory in this master thesis is diffusion theory. Diffusion refers to the process by which an innovation is communicated through certain channels over time among members of a social system (Rogers, 1983). The term was popularised by Everett Rogers in his seminal book *Diffusion of Innovations*, which was first published in 1962. The theory of diffusion is particularly suited for the purposes of this thesis, as it aims to understand the powers that affect the speed with which innovations are diffused, then adopted or rejected, by an audience. The diffusion rate is affected by four elements: the innovation; communication channels; time; and, a social system.

Geroski (2000) synthesises four diffusion models from the vast literature on the subject. These models assume that diffusion follows an S-curve, which refers to the cumulative number of adopters of an innovation over time. Past research generally shows that the adoption of an innovation follows a normal, bell-shaped curve when plotted over time on a frequency basis (shown in Figure 5.1), which, in turn, implies an S-curve (Rogers, 1983).

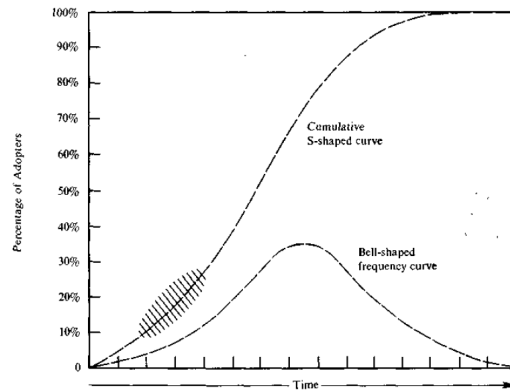


Figure 5.1: The bell-shaped frequency curve and the S-shaped cumulative curve for an adopter distribution (Rogers, 1983)

First, and most commonly found, is the epidemic model, which says that adoption is determined by the lack of available information about a new technology, how to use it and what it does. Second, the probit model says that adoption is determined by firm-specific costs and characteristics: that different firms, with different goals and abilities, are likely to want to adopt new technology at different times. Third, the density dependence model says that adoption is determined by technology acceptance and market saturation, building on concepts such as legitimation and competition to explain the user birth and death rates, ultimately limiting their uptake. Fourth, the technology variant model says that adoption is determined by the decisiveness of choice between variants (Geroski, 2000).

These models are briefly summarised in Figure 5.2.

EPIDEMIC	PROBIT	DENSITY DEPENDENCE	TECHNOLOGY VARIANTS
Adoption is determined by information diffusion .	Adoption is determined by firm-specific costs and characteristics .	Adoption is determined by technology acceptance and market saturation .	Adoption is determined by the decisiveness of choice between variants.
<ul style="list-style-type: none"> - Information - Homogeneity and Proximity - Profits, Learning and Risk 	<ul style="list-style-type: none"> - Firm Size - Suppliers - Costs 	<ul style="list-style-type: none"> - Legitimation - Competition - Pre-emption Effect - Rent Displacement 	<ul style="list-style-type: none"> - Network Externalities - Technical Difference - Bandwagon Effect

Figure 5.2: The four main models of diffusion theory.

Today, smart contracts in its strict sense are poorly diffused in the consumer-facing application space. The wanton diffusion rate will be explored by evaluating the strengths and weaknesses of smart contracts against the models of Figure 5.2, in

order to highlight adoption barriers as well as the potential discrepancies between theory and practice.

5.2 Design Thinking

In 1988, cognitive scientist and usability engineer Don Norman published *The Design of Everyday Things*, which intended to bring a human-centered approach to the development and design of new products and services. By the turn of the century, companies like global design firm IDEO started bringing the succeeding idea of design thinking into business.

Building on a human-centered approach, design thinking is a discipline or methodology that aims to match people's needs with what is technologically feasible and what a viable business strategy can convert into customer value and market opportunity (Brown, 2008). The techniques associated with design thinking (rapid prototyping, empathising, etc.), although they will be implicitly used in the thesis, will not be the subject of further theoretical analysis. However, the idea of three dimensions of product or service value, that is, (1) human desirability, (2) business viability, and (3) technical feasibility, will be used to contextualise the challenges for smart contracts to work in the insurance sector. In other words, the dimensions will be used to create a framework for studying the appropriateness of smart contracts in the case study, when analysing claims flows.

5.3 The Grid

In 2017, business strategist Matt Watkinson published *The Grid*, a framework for analysing key factors in business strategy (Methodical, 2019). Watkinson is the CEO of Methodical, a UX and strategy consultancy based in London and San Francisco. He is also a Senior Visiting Fellow at Cass Business School, London.

The Grid builds on the idea that business success relies on three factors: desirability (i.e. the business solves a problem for the potential customer); profitability (i.e. the business can make a profit solving that problem); and, longevity (i.e. the business can sustain the profit over time). Clearly, these factors are interrelated, as a business cannot have profitability without desirability, or longevity without profitability (Watkinson, 2017).

Moreover, the framework builds on three levels of change that can affect a business: customers (e.g. new behaviours or preferences); market (e.g. new entrants or business cycle shifts); and, organisation (e.g. optimisation and innovation activities) (Watkinson, 2017).

These levels of change interact with each business success factor, which creates nine strategic levers, as shown in Figure 5.3.










	DESIRABILITY	PROFITABILITY	LONGEVITY
CUSTOMERS	WANTS & NEEDS  <input type="checkbox"/> values & beliefs <input type="checkbox"/> goals <input type="checkbox"/> barriers	REVENUES  <input type="checkbox"/> revenue model <input type="checkbox"/> price <input type="checkbox"/> volume (qty & freq.)	CUSTOMER BASE  <input type="checkbox"/> awareness <input type="checkbox"/> acquisition <input type="checkbox"/> retention
MARKET	RIVARLY  <input type="checkbox"/> category <input type="checkbox"/> territory <input type="checkbox"/> alternatives & substitutes	BARGAINING POWER  <input type="checkbox"/> with customers <input type="checkbox"/> with suppliers <input type="checkbox"/> rules & regulations	IMITABILITY  <input type="checkbox"/> legal protection <input type="checkbox"/> durable advantages <input type="checkbox"/> competitor lag
ORGANISATION	OFFERINGS  <input type="checkbox"/> proposition <input type="checkbox"/> brand appeal <input type="checkbox"/> customer experience	COSTS  <input type="checkbox"/> fixed costs <input type="checkbox"/> variable costs <input type="checkbox"/> capital expenditure	ADAPTABILITY  <input type="checkbox"/> cash position <input type="checkbox"/> capacity or scalability <input type="checkbox"/> complexity & rigidity

Figure 5.3: The Grid by Matt Watkinson (Watkinson, 2017).

For the purposes of this thesis, this Grid model has been modified to work as a framework for analysing technology strategy rather than business strategy. Thus, the factor longevity is changed to feasibility, so as to reflect the design thinking principles in full. Figure 5.4 shows how this high-level framework will look.










	DESIRABILITY	PROFITABILITY	FEASIBILITY
CUSTOMERS	WANTS & NEEDS 	REVENUES 	USABILITY 
MARKET	RIVARLY 	BARGAINING POWER 	SUPPORTING INFRASTRUCTURE 
ORGANISATION	OFFERINGS 	COSTS 	KNOW-HOW 

Figure 5.4: The authors' modified Grid model.

This framework will be used to analyse insurance firms' approach to smart contracts in future scenarios based on different degrees of blockchain adoption.

6 Strengths and Weaknesses of Smart Contracts

In this chapter, a description of smart contracts technologies' strengths and weaknesses related to the insurance industry is presented, based on the definition taxonomy and blockchain design choices. A strength/weakness matrix is developed to synthesise the findings. Based on design thinking principles, a checklist is developed for determining the appropriateness of a smart contract solution for a specific claims flow, which is presented in the following chapter.

A systematic process is employed to quantify strengths and weaknesses related to the insurance industry. In order to qualify to each list, a strength or weakness has to be mentioned either in three independent academic papers or two independent interview groups. Since the interviews permit less time for thoroughness and thoughtful consideration, the authors place a somewhat higher value to the few points the interviewee's make. Moreover, the interviewees' backgrounds and perspectives were more mixed. When listed, focus will be on how the strengths or weaknesses interact with opportunities or threats in the insurance market.

Moreover, since there is an overwhelming focus on strict smart contracts both in the literature and in the expert interviews, the first list compiled will focus on the strict definition. When this is done, the traits related to third-party-absence will be re-examined and adjusted for the soft definition. Thus, a new list of strengths and weaknesses is compiled for the soft smart contracts.

Table 6.1 shows the number of times the strengths and weaknesses have been explicitly mentioned in the literature or interviews.

Table 6.1: Smart contract strengths and weaknesses mentioned in articles and interviews.

<i>Strength</i>	<i>Number of explicit mentions in articles (interviews) out of 20 (17)</i>
<i>Fast, automated and low-cost transaction</i>	12 (8)

<i>No central authority needed</i>	14 (4)
<i>Tamper-proof</i>	8 (2)
<i>No single point of failure</i>	7 (0)
<i>Full transparency</i>	6 (2)
<i>Clear rules</i>	5 (2)
<i>Huge information repository</i>	4 (1)
<i>Equal treatment of participants</i>	4 (0)
<i>Cryptocurrency integration</i>	3 (1)
<i>Global reach</i>	3 (1)

<i>Weaknesses</i>	<i>Number of explicit mentions in articles (interviews) out of 20 (14)</i>
-------------------	--------------------------------------------------------------------------------

<i>“Candy” for hackers</i>	9 (1)
<i>Oracle problem</i>	9 (4)
<i>Lack of flexibility</i>	9 (1)
<i>Legal friction</i>	9 (2)
<i>Performance and scalability issues</i>	6 (2)
<i>Malicious or illegal usage</i>	6 (1)

<i>Reducing user privacy</i>	6 (1)
<i>Lack of infrastructure and standards</i>	6 (6)
<i>Over-hyped</i>	5 (6)
<i>Lack of understandability and usability</i>	5 (2)
<i>Government and regulatory unacceptance</i>	4 (4)
<i>Lack of stakeholder adoption</i>	3 (3)

6.1 Strengths

6.1.1 Fast, Automated and Low-cost Transactions

Smart contracts could make the commitment and performance stages of contracting much more efficient. Promising fields of application can be found in areas which allow binary rule schemes to provide fast evaluation and instantaneously generate low-cost insurance (Hans et al., 2017).

Smart contracts are designed to relieve some of the inefficiencies of insurance products, which traditionally are very inefficient with high [operating costs] (Brukhman, 2019).

Since the contract itself becomes the agent which checks and executes its terms, the contract owner does not have to lift a finger once said terms have been agreed upon. This is especially relevant for speeding up claims processing and is accomplished by encoding the rules that enable the transfer of refund from the insurer (or another third-party) to the insured (Gatteschi et al., 2018a).

The generic insurance systems require manual interactions across different transaction processes, hence resulting in slow processing, and lengthy payment settlement time (Raikwar et al., 2018).

Removing humans from many of these processes could reduce the claims handling friction experienced by policyholders (Kruise, 2019). Specific conditions could be

designed to gather information over time to ease the assessment when a claim is filed. A simple example would be triggering an automatic refund only if the customer repairs his or her car at a certified mechanic, with the mechanic sending a transaction to the smart contract to prove its identity (Gatteschi et al., 2018a). This trigger could be twofold: approving a claim only if the certified mechanic has repaired the car, but also if regular check-ups have been done at a certified mechanic since the car insurance was purchased.

There are however some reservations concerning the extent to which claims can be digitally automated:

[It] must be said that the scenario above could be adopted only for a limited number of policies. In fact, the majority of claims processed by insurance companies still need to be evaluated by an external expert before being settled. (Gatteschi et al., 2018a)

This point will be further elaborated on in Section 7.2.

6.1.2 No Central Authority Needed

The essential characteristic of a blockchain is the way in which it enables decentralisation while still solving the double spending problem (Junis et al., 2019). The removal of intermediaries is arguably the most radical aspect of smart contracts, which have historically relied on third-party mediation (Wang et al., 2018). In the strict sense, a smart contract could become a software agent substituting third-parties in a peer-to-peer (P2P) model of transaction that is both scalable and secure (Wang et al., 2018). The smart contract effectively becomes a user interface between negotiating partners, acting “more like apps than contracts, fully collapsing the distinction between agreement formation and execution” (Sklaroff, 2018).

An even more radical take would be the idea that each consumer could be empowered to negotiate online through smart contracts (Fairfield, 2014). By programming the terms of a trade into a smart contract, a consumer could send it scouring the internet for a counterpart willing to trade on those terms. In this way, users would be able to negotiate on terms that are today implicitly decided by corporations: pricing terms, warranties, absence of monitoring individuals’ behaviours online, etc. (Savelyev, 2016). This is already practiced in the second-hand sale of goods, but not in insurance. Additionally, consumers could use smart contracts to participate as investors in these markets (Brukhman, 2019).

6.1.3 Tamper-proof

A strict smart contract is immutable and unmodifiable once created:

[...] since its logic is seeded into a blockchain spread across multiple points. This prevents powerful parties from opportunistically breaching the contract or extracting a beneficial modification that disadvantages weaker counterparties. (Sklaroff, 2018)

In low-trust environments, technically guaranteed data immutability can eliminate the risk of manipulation or other fraudulent practices.

The immutability of blockchain could also become an advantage in countries where censorship is a praxis, as people could publish their thoughts on the blockchain without anyone deleting or changing the text. (Gatteschi et al., 2018b)

Tamper-resistance is inherent in the blockchain technology on which strict smart contracts are usually built (Hu et al., 2019). Even private blockchains, which usually have weaker blockchain-specific benefits than their public counterparts, benefit from this trait compared to traditional centralised databases (Gatteschi et al., 2018a).

For the insurance industry, this is a particularly attractive characteristic in markets where corruption is rampant (Hans et al., 2017) or the market is underserved and would benefit from either auditable third-parties or more peer-to-peer insurance. In high-trust markets, this benefit is less evident:

In Nigeria, you might say it is good to have a blockchain-based land registry, [where] there is nobody to trust: governments are corrupt, locals might be corrupt, even the sellers and buyers might be corrupt. [...] Now, here in Denmark and in Germany, since the 16th century you have had government-run land registries. They work. The government runs them, but I have not heard anybody trying to attack that. (Henglein, 2019)

6.1.4 No Single Point of Failure

Data redundancy is another characteristic of blockchain technology, since each network node has a copy of the distributed ledger. This means that the dysfunction of any one node will not affect the integrity of the ledger, avoiding bottlenecks or data losses (Gatteschi et al., 2018b). Proponents argue that this benefit works even in decentralised autonomous organisations (DAOs) (O'Hara, 2017). But it is important to point out that this is not a blockchain-unique trait. Distributed but third-party-owned databases have been a subject of research for several decades, and have in fact seen increased interest with the blockchain hype (Halaburda, 2018).

6.1.5 Full Transparency

Public blockchains can be inspected by anyone in the world, including not only the final state of transactions but also the history of passed states (Gatteschi et al., 2018b). Given that the person inspecting a smart contract is fluent enough to read the code (Sklaroff, 2018), this ensures that contract terms can be scrutinised more

rigorously than before. Access is always granted immediately, improving auditability by executives, clients or regulators (Hans et al., 2017).

This is of course highly relevant to the insurance industry (Hu et al., 2019) with contract terms that are not always well-understood. Previously, an insurer could decrease transparency either by limiting accessibility to the terms or by intentionally showing misleading terms. With the exception of private blockchains, neither case is possible with a strict smart contract, since the code is the contract. Thus, risks associated with the intermediaries' decision-making and human-factor errors are mitigated (Savelyev, 2016). This could enforce the perception of fairness in claims handling (Nam, 2018).

With that said, there are many ways in which an insurance company can create or increase transparency that does not need to involve blockchain technology. An example would be a soft smart contract that has its terms uploaded on an open source website (e.g. GitHub), where other users would be able to suggest improvements to the contract terms.² Even simpler would be to just have the contract terms on the insurer's own website, but explained in a pedagogical way so that even those not well-versed in code would understand the if-then-statements.

6.1.6 Clear Rules

Smart contracts are codified by nature. This makes interpretation of their terms much simpler than the more fluid and implicit semantic contracts. Smart contract terms are interpreted by machine-based Boolean logic in contrast to classic contracts, which means that the precision of the programs can mitigate issues associated with unpredictable interpretation of contractual terms by contract parties or adjudicators (Savelyev, 2016). The benefits manifest in both better fraud prevention and fewer legal disputes, as the terms of agreement are clearly decided beforehand (Gatteschi et al., 2018b). Wosa (2019) argues that the removal of disputes and resolution in contracting is a key benefit of strict smart contracts. For policyholders, it would also create a better understanding of exactly which events lead to which outcomes (Kruuse, 2019).

6.1.7 Huge Information Repository

Should blockchain technologies be more widely adopted, it would be possible to build identity and content chains which host huge datasets from a wide range of sources (Hans et al., 2017). How private or public these chains are become a matter of infrastructure and standards. The practical use of such repositories is of course

² The American insurtech Lemonade is piloting this concept through its Policy 2.0.

endless. In insurance, it would contribute to improved risk assessments and premium calculations as well as fraud prevention (Gatteschi et al., 2018a), which could be built into even smarter smart contracts — less reliant on proxies and unreliable oracle data.

6.1.8 Equal Treatment of Participants

Smart contracts, even in the soft sense, can contribute to an egalitarian approach to claims handling. This benefit is most pronounced but not exclusive to a public blockchain (Hans et al., 2017). Instead of human judgement based on individual discretion and bias, a codified contract could systemise the rules for payouts to apply for all claimants.

Moreover, those rules could be openly communicated to allow for scrutiny and revision, should they be considered poorly designed. This is an important point to note, as a codified program carries the bias of its designer with it. The choice of oracles, proxies and other decision-driving data sources should all be done with great care.

An issue related to this is that smart contracts will lack reasonable weak party protection, since everyone is treated equally. But this could be outweighed by more bargaining power:

[...] Smart contract architecture does not allow to ensure protection of weak parties, e.g. consumers. The whole layer of legal provisions relating to consumer law and unfair contract terms is non-applicable to [a] Smart contract. At the same time, Smart contracts may provide some extra leverage for consumers to protect their interests. Currently consumers don't have any realistic choice as to conclude or not to conclude a contract: they don't have time to read the terms and conditions, and even if they do — they don't understand its terms. Even if an individual understands them, he does not have bargaining power to change them and if he decides to go to another seller — the outcome will be the same. Smart contracts allow using electronic agents for conclusion of the agreement, and potentially they may be programmed in a way allowing them to search favorable terms and even negotiate them within the established boundaries. (Savelyev, 2016)

All well-designed and openly communicated rules-based systems of claims management would greatly contribute to the perceived fairness of the insurer (Nam, 2018).

6.1.9 Cryptocurrency Integration

Strict smart contracts are especially useful on blockchain platforms with their own native cryptocurrency, or which are cryptocurrency compatible. Transactions could be faster:

In case of manual [claims] processing, however, the customer experience could still be improved by managing payments in cryptocurrencies, whose transfer would be quicker than with traditional methods (several seconds or minutes depending on the blockchain used). (Gatteschi et al., 2018a)

Since cryptocurrencies like bitcoin and ether work on-chain, the need for banks and other institutions is removed (Sklaroff, 2018). Thus, costs related to such institutions (e.g. bank commissions or overseas transfers) could also be lowered or removed in their entirety.

Transactions would be less reliant on unsecure off-chain IT systems. Halaburda (2018) argues that the key benefits of blockchain are only realised with the use of native cryptocurrency:

[...] benefits may be difficult to realize in a blockchain without Bitcoin. It has proven to be a challenge to create a decentralized, permissionless and secure blockchain to transfer assets other than a native cryptocurrency (for example, bitcoins for the Bitcoin blockchain). [...] The network participants are rewarded for their costly work with bitcoins. Without bitcoins (or other native cryptocurrency), the network participants need to be motivated by incentives from outside of the blockchain. (Halaburda, 2018)

In fact, Halaburda (2018) goes on to state directly that:

[...] we need to realize that outside of Bitcoin (or other cryptocurrencies) we do not have a technology that offers “permissionless distributed ledgers that cryptographically assure immutability without a need for trusted third parties.” (Halaburda, 2018)

Using cryptocurrency could guarantee the anonymity of the user in a way which has been previously impossible. Trustless public ledgers combined with native cryptocurrency can remove a major source of consumer hesitancy and complexity in using consumer-driven automated agents by eliminating the need for consumers to entrust those agents with personal information (Fairfield, 2014).

It is evident that many of the great benefits of strict smart contracts, or in general blockchain solutions, rely on cryptocurrency integration.

6.1.10 Global Reach

Data that is stored on a blockchain can be both accessed and tracked worldwide, not unlike the internet. Material assets such as luxury items or immaterial ones like intellectual property can be traced due to this transnational characteristic (Gatteschi et al., 2018b).

Furthermore, blockchain use could accelerate the globalisation of insurance and create new markets that add substantial value for consumer-facing applications:

You can have cheaper and more granular insurance. The markets of risks open up and become available to more investors globally. The reinsurance markets open up more. More insurance is more liquid. (Brukhman, 2019)

In the long term, it could contribute to more standardised systems of record-holding, which could underpin globally enforceable and controllable strict smart contracts. However, as will be shown, it also creates legal headaches.

6.2 Weaknesses

6.2.1 “Candy” for Hackers

Because of the data immutability of strict smart contracts, any bug or weakness found after the launch of the contract on the blockchain cannot be remedied. This means that hackers that are interested in exploiting errors can easily do so post-launch, even if the contract programmers realise their mistakes.

Developing a safe Ethereum smart contract program is challenging because of the nature of its immutability, early ecosystem development, and a high incentive to be hacked as it can store economic value. (Junis et al., 2019)

This puts pressure on developers to ensure that their contracts are completely waterproof before launch, which increases development and negotiating costs. The difficulty of writing smart contract code endangers the security of contracts (Alharby & van Moorsel, 2017).

The most notorious example of a successful attack is the 2016 attack on a DAO named *TheDAO*, a self-managed capital investment fund run on peer-to-peer strict smart contracts. A third of its value was siphoned off through a replay attack in which the same transaction was repeated over and over again, amounting to roughly \$55 million at the time (O’Hara, 2017).

The severity of this issue is reflected in the literature’s frequent focus on it. A 2017 study by Alharby and van Moorsel (2017) found that out of 24 surveyed papers on smart contracts, two-thirds of them described the technology’s issues and suggested solutions to them. Mentioned security issues include transaction-ordering dependency (TOD) vulnerabilities, timestamp dependence vulnerabilities, mishandled exception vulnerabilities, and reentrancy vulnerabilities (e.g. TheDAO attack) (Alharby & van Moorsel, 2017). While some of these issues have been addressed and solved, the risk of bugs is always present — and ready to be exploited. Many vulnerabilities stem from a misunderstanding of the scripting languages (Hu et al., 2019).

6.2.2 Oracle Problem

Many insurance contracts would need to inject data from external sources, which creates another weakness in the contract (Gatteschi et al., 2018a). In the strict smart contract sense, an oracle could remove the entire point of having a blockchain, since the external data is not subject to the same consensus protocol which guarantees the trustworthiness of on-chain transactions (Wang et al., 2018). This issue becomes evident when considering the fact that the Bartoletti and Pompianu (2017) study of existing strict smart contracts showed that only 7% employed an oracle, while the rest relied only on on-chain information. This suggests that contract designers might be struggling with finding and securing proper oracles.

Even in the soft sense, the quality of oracle data is a major concern. Any data fed from outside parties cannot be fully trusted (Hu et al., 2019). Oracles are effectively the judges of how and when contracts should be executed. When a smart contract relies on them, it loses “having the last word” (Wain, 2019). Thus, the reliability of oracle data is paramount. Several issues can be identified, which are collectively described as the oracle problem or gateway problem (Halaburda, 2018). First, there could be insufficient oracle data; simply, a lack of sources necessary. Second, the oracle data could be faulty which effectively eliminates the *raison d'être* of the smart contract. Third, the oracle data could be intentionally manipulated to affect the outcome of a contract. Fourth, a reliable or trustworthy oracle could disappear or stop functioning for some reason during the lifetime of the contract (Hans et al., 2017).

What is problematic for me is that I cannot find any applications where oracles exist. If I had oracles, I would gladly have self-enforcing contracts. (Valentin, 2019)

Some signature concepts such as having “three out of five” oracles confirming a data point have been installed to reduce these risks (Hans et al., 2017).

Today, the oracle makes the least secure part of the smart contract, but there are a number of critical developments in progress that could make oracles more trustworthy in the future (Lennyi, 2019)

6.2.3 Lack of Flexibility

Paradoxically, there are some major drawbacks related to the major benefits of blockchain-based smart contracts. The data immutability or tamper-resistance of strict smart contracts also create an inflexibility that can be quite costly and impractical (Sklaroff, 2018). This is ironic, considering that efficiency is the ultimate pursuit of those who wish to automate and digitalise paper-based or semantic contracting:

When smart contract proponents dismiss traditional contracting for being too unpredictable, messy, or time-consuming — in other words, for being too human — they overlook the reality that every transaction and every set of trading partners is unique. Each grapples differently with the challenge of fully-specifying performance ex ante and the pressure to informally modify agreements. Contractual flexibility, driven by the richness of semantic expression and the power of human judgment, provides an efficient way to manage those costs. (Sklaroff, 2018)

There is no way to patch a buggy smart contract, regardless of its popularity or how much money it has, without reversing the blockchain, which is practically impossible (Luu et al., 2016). More importantly, it is actually frowned upon by a large portion of the blockchain community, which consider the code to be law (O’Hara, 2017). Even if the parties involved would like to change or modify their agreement:

[...] fully decentralized blockchains are by design able to hinder any kind of non-mutual and external intervention, no matter if legitimate, desirable or necessary to enforce basic safeguards or mandatory norms. (Cuccuru, 2017)

Going back to the strength in clear rules, it becomes evident that the *ex post* benefit of less litigation and fraud is counterbalanced by the *ex ante* cost of inflexibility — the need to have a “perfect” contract before launching it.

More specifically, some effective human concepts are lost in translation; the entire contract has to be explicitly described rather than implicitly understood. One example of this is the fairly common business practice of voluntary breach of an agreement (Cuccuru, 2017), in which a party agrees to carry the cost of contract breach because his or her funds can be better spent elsewhere. There are several such implicit general standards and business praxes which are diffuse and thus difficult to encode (Cuccuru, 2017).

Ethereum founder Buterin (2014) argues that flexibility could be added to smart contract design as well:

Although code is theoretically immutable, one can easily get around this and have de-facto mutability by having chunks of the code in separate contracts, and having the address of which contracts to call stored in the modifiable storage. (Buterin, 2014)

Nonetheless, there is complexity and obscurity in this way of designing contracts.

6.2.4 Legal Friction

Savelyev (2016) argues that what strict smart contract developers are doing is creating a technical universe “parallel” to the legal realm, without a backward glance to any legal considerations, not unlike the early days of the internet:

[A] computer is indifferent to the fundamental legal principles, such as lawfulness, fairness, protection of weak party. Instead the principles of certainty and effectiveness prevail. (Savelyev, 2016)

In fact, smart contracts are not legally binding in a technical meaning (Cuccuru, 2017). It goes without saying that this creates all kinds of problems. For one, legal law allows for rules to be modified, breached or terminated (Alharby & van Moorsel, 2017). But notwithstanding problems related to traditional lawfulness, national borders and jurisdiction, lack of human and semantic flexibility in contracting, or disintermediation of legal entities, there is the fundamental idea that the code is law. What this means is that the code, with all its flaws and legal shortcomings, is still what should hold as the agreed-upon document. Going back to the TheDAO attack, this principle was certainly put to the test. In that situation, when it really mattered, the Ethereum coders decided to revert to a personal sense of what was fair rather than what was sanctioned by code:

Fortunately (depending on your point of view) the hack required the money to be siphoned off into a subsidiary bank account where it sat for long enough for Ethereum's coders to devise and implement a hard fork to recover the cash and restore it to the investors [...]. (O'Hara, 2017)

But this failure of principle just shows the complicated reality of law and fairness. By creating a controversial fork in the blockchain (Wang et al., 2018), they broke the basic rules of the game:

Recall, The DAO was premised on smart contracts, whereby the code is the contract. The contract therefore couldn't be rescinded, and trust in the system wasn't needed — such was the rhetoric. Yet in the face of a loss that used the code as written, the smart contracts were indeed rewritten. (O'Hara, 2017)

These forks spark intense disagreement in the blockchain community not only because they change the law after-the-fact, but because they represent a majority-rule approach to changing the rules of all contracts in the system (Sklaroff, 2018). According to the code is law principle, the hacker who siphoned TheDAO is the rightful owner of the money stolen and could actually have a claim to the money that was returned to investors through the hard fork. In fact, the attacker claimed as much in an open letter to the Ethereum community, stating that he had not done anything illegal, but was only “making use of this explicitly coded feature as per the smart contract terms” (Savelyev, 2016).

6.2.5 Performance and Scalability Issues

The existing strict smart contracts are comparably few, arguably insignificant, to the existing pool of non-smart contracts in the world. Thus, a discussion regarding the scalability and performance of blockchain-based solutions is in order. There seems

to be severe limitations to high-performance at scale (Arden, 2019). Strict smart contracts are characterised by high power consumption. Moreover, mining requires expensive hardware while the majority of computer power is wasted on calculations that do not result in anything (Gatteschi et al., 2018b). Proof-of-work is quite an inefficient consensus mechanism, not only in terms of electricity, but also speed (Halaburda, 2018). Changing the consensus mechanism, for example from proof-of-work to proof-of-stake, could improve these weaknesses (Gatteschi et al., 2018b).

Since each network node stores a local copy of the blockchain, which requires considerable storage space, performance is not yet comparable with databases (Gatteschi et al., 2018b). This is further complicated by the fact that the entire transaction history is saved rather than just the current balance (Halaburda, 2018).

Also, the number of transactions which can be handled per second is extremely low compared to traditional systems. Although the speed is sufficient compared to traditional bank transfers, it is not up to the task for instant payments or similar applications (Gatteschi et al., 2018b). Moreover, the sequential execution of contracts sets a hard limit to the speed with which contracts can be processed, unless the consensus protocol is simplified, which risks removing the other benefits of blockchain (Alharby & van Moorsel, 2017).

Another obstacle which inhibits scalability is interoperability with legacy systems (Hu et al., 2019). This is especially inhibiting for the early adoption of blockchain-based systems, as the legacy cannot be thrown out the window in one move.

Concluding this, Halaburda (2018) argues that a strict smart contract only makes sense where the reconciliation of contradictory ledgers is prohibitively costly and a centralised solution is untrustworthy:

To date, it has not been clearly demonstrated in which circumstances the benefits of employing a distributed ledger outweighs the cost of delays and duplicated storage. (Halaburda, 2018)

6.2.6 Malicious or Illegal Usage

While the consensus protocols are designed to discourage malicious usage, there are many bugs and other security issues to exploit, as previously described. Another dimension is actively illegal usage which in many ways is supported by the fundamental structure of blockchains with native cryptocurrencies:

The high level of privacy protection offered by the decentralized architecture has from the beginning raised serious concerns as regards the use of Bitcoin for illicit activities, money laundering, tax evasion, fraud and trade in illegal goods, among others. (Cuccuru, 2017)

Smart contracts treat legal and illegal subject matters in the same way, as long as it is codifiable (Savelyev, 2016). This has caused a great deal of debate about the potential illegal uses of cryptocurrency, for example for procuring hacker services by offering a cryptocurrency reward (Savelyev, 2016).

Additionally, it is worth noting that some activities which are considered criminal by law are not necessarily accepted as such by influential voices in the blockchain communities. There is an anarchistic streak, especially in the Bitcoin but also Ethereum community, which argue that a government has no moral authority to pass judgement on what is or is not moral behaviour (Henglein, 2019). As such, activities like money laundering need not be considered a problem in need of solving by many of the influential blockchain technologists, who would more likely object to the negative connotation implicit in the expression “money laundering”.

6.2.7 Reducing User Privacy

There seems to be some confusion in the literature whether blockchain technologies in fact reduce or increase privacy (Halaburda, 2018). Transparency is described as an essential part of strict smart contracts, which implies the visibility and openness of everything from contract terms to personal transaction records, since network nodes store a local copy of the blockchain.

In blockchain systems, all transactions and users' balances are publicly available to be viewed. (Alharby & van Moorsel, 2017)

This sort of transparency could harm the users' privacy and reputation (Gatteschi et al., 2018b). Still, Hans et al. (2017) argue that anonymity can be achieved by using different blockchains for different types of data: identity, transaction, and content chains.

How exactly this would work is less clear. Halaburda (2018) suggests that privacy stems from cryptographic measures and their continued improvement rather than something inherent in blockchain. While users can counterbalance the transparency of the blockchain with pseudonyms (which makes it difficult to link a blockchain account to a person's real identity), traceability through “indirect means of control” cannot be avoided unless the user turns to more “resilient anonymization services” (Cuccuru, 2017). While hackers and others interested in illegal or malicious usage of blockchain might be familiar with such anonymisation services, many common users are not.

The huge repository of data that is created by a blockchain, paired with privacy concerns, demand new structured approaches for the development of blockchain designs (Hans et al., 2017), or greater reliance on cryptocurrencies.

Another important aspect, related to the aforementioned legal friction, is new data protection and privacy regulation, such as Europe's GDPR, or General Data

Protection Regulation. Laws such as GDPR, or more generally the right to be forgotten, which are built on the idea of having a data controller, are naturally not supported by blockchain technologies (Lindman, 2019).

6.2.8 Lack of Infrastructure and Standards

A temporary weakness in the technology is its own immaturity. A prime example of this is the absence of internet of things (IoT) diffusion, which is likely to change in the coming years. With a broad infrastructure of physical sensors, it is more likely that the benefits of soft smart contracts will be realised. However, even then, insurers would have to agree on how to codify liability based on sensor data, which is another dimension of standard setting that will become more relevant in a connected IoT world (Valentin, 2019).

Because of this and other similar infrastructure deficiencies, Savelyev (2016) argues that it would not be correct to conclude that smart contracts are by default cheaper than regular ones. Costs associated with the development, or drafting, of smart contract terms are still rather high (Savelyev, 2016).

Moreover, a lack of formalised ways for creating smart contracts to suit various design purposes, especially when there are legal components involved, inhibits wider adoption in business procedures (Hu et al., 2019). Wain (2019) argues that office politics and organisational inability to agree on common protocols are essential barriers for private blockchain adoption. Lindman (2019) points to the lack of tooling (i.e. programming languages, documentation, education, building blocks) as a main barrier for building strict smart contracts. This will no doubt be developed over time, since there are expert councils already working on such standards (Henglein, 2019). Moreover, some companies are competing to be the first to create a standard for translating semantic contracts to digital ones (Crillesen, 2019). Developing smart contract user interfaces and assigning internal responsibility for managing them will be essential (Arden, 2019).

Finally, the lack of a dominant technology variant might cause hesitation in firms that are interested in investing in blockchain. This is evident in the proliferation of blockchain platforms. While Ethereum is the most popular smart contract platform in terms of the number of contracts running on it, Bitcoin contracts process higher transactions amounts in total, not to mention the existence of smaller platforms like Counterparty, Monax, Lisk, Hyperledger Fabric, Corda, Bigchain DB, Neo, EOS and others which have their own benefits and drawbacks for different types of smart contracts (Bartoletti & Pompianu, 2017; Wang et al., 2018; Hu et al., 2019). Crillesen (2019) highlights the associated risk with this from a business perspective:

[...] generally, for large companies, there's a huge leap when undertaking this kind of technology, because there's a large upfront cost and insecurities and uncertainties about whether the technology will work and who can manage it. (Crillesen, 2019)

6.2.9 Over-hyped

Blockchain is an incredibly hyped technology. For the insurance industry, the technology is still considered to be in an innovation trigger phase, meaning that “the spectrum of possible applications has not been fully explored yet” (Gatteschi et al., 2018a). While there is an increasing awareness of this fact within the literature, there are still many papers which uncritically espouse the potential benefits of smart contracts without describing how they will be realised (Halaburda, 2018). Moreover, many neglect the fact that a great deal of those benefits can be accomplished with existing or otherwise available technology systems that are not as difficult to implement (Gatteschi et al., 2018b). One example of this is the well-researched field of distributional databases (Halaburda, 2018). These might not be concerns when theorising about the potential in blockchain, but it certainly affects the pace of adoption in the market.

A particularly fascinating aspect of this hype relates to the design of blockchain systems. More specifically, the choice between having a public or private and permissioned or permissionless blockchain system. Many of the benefits that are unique to blockchain technology are really dependent on a public and permissionless structure. Some of the drawbacks of blockchain can be solved with a permissioned structure, at the cost of reducing its benefits. Examples include challenges such as the oracle problem as well as performance and scalability issues (Halaburda, 2018):

In most of the currently proposed applications, both challenges have been addressed by creating closed, permissioned blockchains. This is because a blockchain without bitcoins is no longer virtually immutable without a trusted third party. In many cases, permissioned blockchains are the right tools for their purpose. We need to recognize, however, that they depart from Bitcoin’s innovation. They effectively go back to the traditional concept of distributed databases. Moreover, if permissionless is not the goal, then we need to consider whether a blockchain [...] is the optimal design choice for those permissioned distributed databases. (Halaburda, 2018)

Moreover, Hans et al. (2017) note that a permissioned design with known identities makes a consensus model unnecessary (thus increasing performance) but decreases the degree of data transparency. This sort of paradoxical relation in the benefits of permissionless and permissioned designs weakens the supposed benefits of blockchain from an insurer’s perspective.

6.2.10 Lack of Understandability and Usability

There is some disagreement regarding the understandability and usability of blockchain technology. On a fundamental level, the technology set-up for a regular user need not be too complicated to understand (Lindman, 2019). While few people can describe the architecture or logic behind the internet, most people in advanced

economies still know what it can do for them and what they need to set-up in order for it to work (Henglein, 2019). To set up a wallet and operating it, a user does not need to understand the consensus mechanisms (Lindman, 2019). This is, of course, also a matter of which adoption category an individual falls into; early adopters being more prone to test unproven or unconventional technologies (Rogers, 1983).

But the problem is nonetheless manifold. First of all, it is difficult to understand what is needed to start trading with the existing smart contracts on a blockchain, not to mention setting up your own smart contract. This is further complicated by the sometimes-unintuitive terminology that has become standard within the blockchain literature (Henglein, 2019).

A considerable issue relates to code literacy. One of the primary promises of strict smart contracts is full transparency, but it does not matter that anyone can inspect such a contract if no one is literate enough to understand its contents:

[...] user-friendly interfaces cannot really eliminate the semantic barriers, but only cover up smart contract technicalities. Indeed, to rely on computer automation for the execution of online agreements [...] ultimately implies computing skills most people — lawyers included — do not have. Non-trained actors [...] would, therefore, struggle to assess the concrete operativity and the full consequences of the (computer) terms they are dealing with. (Cuccuru, 2017)

This would push individuals to seek potentially expensive help to read and write contract algorithms, which, instead of simplifying contracts, would effectively put intermediaries (i.e. points of failure, and trust) back into online relationship management (Cuccuru, 2017; Kruuse, 2019).

This opens up the system to all kinds of exploitation, not just of bugs but of people too unaware or unknowledgeable to recognise fraudulent or unconscionable contract terms (Sklaroff, 2018). Contract terms, which have traditionally been policed by courts, will thus likely “proliferate as ‘code-savvy parties’ take advantage of the ‘code-naive’” (Sklaroff, 2018). The technical complexities of smart contract architecture, which oftentimes requires advanced programming skills that only specialised companies can deliver to clients, will furthermore increase the discrepancy between “the person programming the code and the person intending to use it in commercial activities”, which increases the “risk of misunderstanding between them with regard to the terms of the future agreement” (Savelyev, 2016).

The importance of understandability is further strengthened in an environment where third-party regulation and oversight is weakened, which is the case for blockchain. The consumers must protect themselves. This relates to the legal frictions described before:

In the first place, the law can be challenged, whereas in software the forbidden option is irreversibly grayed out and inaccessible. Second, the law is developed and administered transparently by our democratically elected representatives and the courts; software development, even open source, is opaque, and concentrated in a

small programming community, many of whom are in the pay of a few oligopolistic corporations directly accountable to no external party. (O'Hara, 2017)

And while the focus here has been on the consumer, it is worth noting that similar problems affect programmers of strict smart contracts. In fact, “many vulnerabilities are caused by the misunderstanding of the scripting languages” (Hu et al., 2019):

Scripting languages need to be regulated in a way to be more comprehensive and easy-to-use for both technical and non-technical people. (Hu et al., 2019)

This issue has resulted in some outrageous outcomes. One example is when a GitHub user named *devops199* — a novice experimenting with public Ethereum smart contracts — accidentally terminated a contract containing roughly \$300 million (Yuan, 2017).

Usability issues come in other forms as well. For example, the third-party-absence of blockchain platforms make it impossible to receive assistance in case of credentials loss, unless some reliance is made on trusted services (Gatteschi et al., 2018a).

6.2.11 Government and Regulatory Unacceptance

Given the wide range of issues and concerns which envelop blockchain technologies, and in them strict smart contracts, it is little surprise that governments and regulators (conservative and cautious by nature) have been exhibiting reluctance or even outright unacceptance of these new technologies, considering that even the market shows some signs of distrust and might perceive the technology as unsecure or unreliable due to bugs, cryptocurrency volatility, and more. (Gatteschi et al., 2018a). Arden (2019) and Brukhman (2019) point to this as a central barrier for adoption.

Legal friction and the lack of subsequent regulation and policies make it hard for blockchains and strict smart contracts to obtain government approval. This needs to be a careful consideration for businesses evaluating the opportunities presented by such technologies (Hu et al., 2019).

6.2.12 Lack of Stakeholder Adoption

Related to government and regulatory unacceptance is the general lack of adoption by the stakeholders that make up the blockchain ecosystem. Some of the benefits of strict smart contract, for example access to the huge information repository that blockchain could become, relies on the involvement of a wide array of companies, agencies, users and more, for data. Clearly, this reflects a lack of understandability

and usability as well as the misconceptions and over-hype of the technology (Hu et al., 2019), as previously mentioned:

Even with proper use cases, it can be hard to persuade stakeholders and users to accept the new technology. This could result in extra development costs and a low return on the investment. Some of the proposed use cases are in fact more efficient to implement via traditional databases. (Hu et al., 2019)

As previously mentioned, the lack of interoperability with legacy systems further decrease the likelihood of stakeholders to adopt the technology (Hu et al., 2019). Additionally, there is the general inertia of insurance incumbents, which in the interest of guarding their market position might be hesitant or even actively undermine new technologies that could give new entrants an upper hand (Valentin, 2019).

Finally, there are also consumer network effects present, especially in public blockchains (Wain, 2019). This means that the value of using blockchain platforms increases markedly with every additional user, which might inhibit traction in the beginning but also promises faster growth at a certain point of “critical user mass”.

6.3 The Strict Case

A summary of the above-mentioned strengths and weaknesses can be seen in Figure 6.1. Many of these are directly related to a public and permissionless blockchain design (Lindman, 2019; Crillesen, 2019). Some of the uniquely blockchain benefits (e.g. tamper-proof, no central authority needed) disappear if a permissioned design is adopted, which is the case for many business applications including insurance (Hu et al., 2019). A permissioned design is often necessary to avoid some of the major drawbacks (e.g. lack of flexibility, performance and scalability issues) of the strict smart contract (Halaburda, 2018).

Nevertheless, if on the one hand the ‘privatization’ of the blockchains may grant them a kind of ‘structural’ legitimacy — avoiding the ‘regulatory nightmare’ they potentially pose — on the other it inevitably puts points of vulnerability back into decentralized architectures. (Cuccuru, 2017)

Thus, there are today few permissioned blockchain-based insurance applications that go beyond a proof-of-concept stage (Wain, 2019).

STRENGTH	WEAKNESS
<ul style="list-style-type: none"> • Fast, automated and low-cost transactions • No central authority needed • Tamper-proof • No single point of failure • Full transparency • Clear rules • Huge information repository • Equal treatment of participants • Cryptocurrency integration • Global reach 	<ul style="list-style-type: none"> • "Candy" for hackers • Oracle problem • Lack of flexibility • Legal friction • Performance and scalability issues • Malicious or illegal usage • Reducing users' privacy • Lack of infrastructure and standards • Over-hyped • Lack of understandability and usability • Gov't and regulatory unacceptance • Lack of stakeholder adoption

Figure 6.1: Strengths and weaknesses of strict smart contracts.

Delving deeper, some of the key value-adding aspects of a strict smart contract are only realised in markets with exceptionally low trust or access, for example due to rampant corruption, fraudulent business practices or lacking availability of financial capital and support. These are issues related to fairness:

If you look at smart contracts as purely efficiency tech, then no, efficiency solutions do not have to be on a blockchain. You must use the value proposition of blockchains (i.e. security, privacy, censorship-resistance, openness of platform, openness of the marketplace) in order for blockchain tech to make sense in this context. There are definite advantages to decentralization/trustlessness but they are localized. Censorship-resistance is useful in oppressive countries. Openness of investment opportunity is used in contexts where consumers do not have the power to invest. Global availability means that people without a lot of infrastructure (like the unbanked) can participate. (Brukman, 2019)

This is not the case in digitally mature and institutionally democratic markets like those in the Nordics. While customers might value increased transparency, there is a basic level of trust in third-parties, be they financial institutions or private insurers (Henglein, 2019; Nelander, 2019). If an insurance institution has a strong brand that can emulate trust and qualify as a legitimate arbitrator, then a centralised smart contract is fully possible. In fact, it would be much cheaper (Lennyi, 2019). There is also extensive financial capital and proper access to insurance. Thus, the value of full transparency or third-party-absence as well as global reach is less evident in these cases (Lindman, 2019).

Today, insurance use cases where blockchain-based technologies add significant business value remain unclear; the value is most obvious for financial transactions

services (Arden, 2019). For insurer strict smart contracts, it is still intangible (Crillesen, 2019). In fact, the excitement for the technology often lies beyond the business applications:

I usually do not recommend companies to use blockchain. If I do, there needs to be very specific use cases where you clearly see that [the client] can capture a lot of value from the technology. What I look forward to regarding blockchain is not to empower companies, but rather to disrupt economic systems and markets, which today rely on big companies [...]. (Fred-Ojala, 2019)

Another aspect is that of cryptocurrency integration, which while an interesting invention is still subject to huge volatility and government unacceptance. This not only limits the benefit of having blockchain-based smart contracts, but also risks eliminating the incentive structure that underlies the consensus mechanism (Halaburda, 2018).

Finally, the benefit of having a huge information repository hinges both on broad stakeholder adoption (which has yet to happen) and guarantees of user privacy protection. These are not challenges that are impossible to solve, but goes to show that many of the benefits related to blockchain-based technology have certain pre-conditions which limit adoption speed.

Considering all this: is a blockchain-based smart contract attractive for insurance? On a structural level, possibly:³

The constraints of the digital environment and the concerns surrounding fully decentralized architecture push — at least at this stage — the commercial application of smart contracts towards a well-confined area. Indeed, the boundaries just drawn roughly delimit a field characterized by (i) standardized terms and (ii) measurable — ie easily enforceable by computers — conditions (iii) embedded in a hybrid technological architecture which maintains a certain degree of decentralization while ensuring regulability and room for intervention. It comes as no surprise, therefore, that among blockchain's foreseeable fields of application the most immediate is commonly acknowledged to be [the] financial sector. (Cuccuru, 2017)

With that said, it seems unlikely that the insurance industry will broadly adopt strict smart contracts built on blockchain technology anytime soon, due to the limited value creation for customers and the considerable feasibility and profitability challenges inherent in it.

[...] the current form of [strict] smart contracts are still limited in their ability to fulfill all expectations. (Hu et al., 2019)

³ Disregarding the conservative culture that is typical of insurance.

However, some of the characteristics outlined by Cuccuru (2017) make the insurance industry an exceptionally good fit for soft smart contracts.

6.4 The Soft Case

Soft smart contracts are much more promising than their strict counterparts, when focusing specifically on its potential business value in insurance. While the blockchain-unique benefits are not present⁴, the benefits that are potentially most value-adding in a digitally mature market (e.g. fast, automated and low-cost transactions, equal treatment of participants, clear rules) are still delivered. Moreover, with the right communication strategy, an insurer could achieve something resembling full transparency (or close enough) and, with the right IT architecture, also avoid single points of failure.

STRENGTH	WEAKNESS
<ul style="list-style-type: none"> • Fast, automated and low-cost transactions • No single point of failure ⁽¹⁾ • Full transparency ⁽²⁾ • Clear rules • Equal treatment of participants 	<ul style="list-style-type: none"> • "Candy" for hackers ⁽³⁾ • Oracle problem • Legal friction ⁽⁴⁾ • Reducing users' privacy ⁽⁵⁾ • Lack of infrastructure and standards ⁽⁶⁾

Figure 6.2: Strengths and weaknesses of soft smart contracts.⁵

Some of the biggest issues related to smart contracts apply to both the soft and strict version. Many of them, however, are slightly eased in the soft sense. A major problem is the exploitation of bugs in the code, or loopholes in the logic, which would help hackers and fraudsters earn refunds unfairly or illegally. This needs to be considered deeply when writing code, but in the soft smart contract there is at least wiggle-room to adjust or modify code post-launch, which lowers the risks considerably. In the case of strict smart contracts, once the contract is launched on the blockchain, it is practically immutable.

⁴ Remember that those benefits barely held the test even in the strict case.

⁵ NOTES: (1) Can be built using distributed database; (2) Can be partially built using GitHub or on-site info; (3) Hacking is still a risk — but at least bugs can be fixed; (4) "Code is Law" principle still holds; (5) In the sense that personal data can be used; (6) Still lacks physical sensor infrastructure

A similar discussion can be had about legal friction. In a soft smart contract, the ‘code is law’ principle still holds to a certain degree. The difference is that the code is more localised and modifiable. It is easier to reduce the friction between the technical and legal spheres when a third-party (e.g. an insurer) can control how the terms and conditions are defined.

The key issue that is as severe for soft smart contracts as it is for strict ones, is the oracle problem. A soft smart contract still relies heavily on trusted sources of external information. As has been described, many challenges relate to this problem. But it is not unsolvable, and more importantly, not static.

As for the remaining weaknesses, they affect adoption speed but are unlikely to do so to a prohibitive degree. Standards and infrastructure will be developed over time, for example with the increasing prevalence and integration of IoT solutions. Privacy issues with their all-encompassing reach will be dealt with in one way or another. The internet is not going anywhere, and the same cryptographic standards and consumer protection laws that are applied to that sphere can be applied to soft smart contracts as well.

Finally, it is not necessary for this sort of technology to be relevant for all business processes. With that said, some time should be spent testing which application areas are best suited to maximise the benefits of soft smart contracts. Moreover, while the focus on this thesis is on B2C applications, it is worth pointing out that B2B could be the faster sphere of adoption:

Usually, certain technology becomes routine when technological elite becomes bored with it, after that it becomes mass market. In any case, it is likely that on initial stages Smart contracts will mostly exist in B2B and C2C sectors, but not in B2C segment of e-commerce. (Savelyev, 2016)

7 Case Study: Hedvig Applications

In this chapter, Hedvig is explored as a testbed for smart contract applications in insurance. This is done by looking at both existing insurance products and potentially new ones. Existing claims flows are assessed based on a checklist. A technical schematic is developed as a proof-of-concept (i.e. prototype) for a new insurance smart contract.

7.1 What Have We Learned?

Smart contracts could create value in consumer-facing insurance applications, particularly claims management, which will from now on be the primary area of study. For the Nordics — a market characterised as digitally mature and institutionally democratic — the main benefits of blockchain-based smart contracts are lost, at least in the short- to mid-term.⁶ Thus, focus should be on soft smart contracts and their (1) user desirability, (2) business viability, and (3) technical feasibility for certain claims flows. The strengths and weaknesses previously noted can be translated into key assumptions across these three dimensions of product-market fit. Such a checklist has been developed and is shown in Figure 7.1. What is important to note is that while the assumptions related to viability and feasibility are relatively probable to hold true, the desirability assumptions require extensive experimentation to validate. Such validation has been beyond the scope of the thesis project. As such, the checklist must be seen as a draft version, subject to future amendment. Nonetheless, it is used in this chapter to give an idea of how it can work as a framework for quickly evaluating smart contracts' fit for a certain claims flow.

⁶ In a long-term perspective (10+ years), too many factors are subject to change to confidently reject the relevance of blockchain. As was shown in Chapter 6, the strengths and weaknesses interact with several important (non-static) market forces.



DESIRABILITY

- The smart contract (SM) **increases peace of mind**. ★
- The SM **reduces inconvenience and time effort**. ★
- The SM **increases the speed of refunds**.
- The SM can **embed costs** on the condition of profit.
- The SM operates in a **low-trust environment**.
- The **claim** is a **common occurrence**.
- The **claim** relates to **low- to medium-cost damages**.
- The **claim** is **uncovered or underserved** right now.
- The **claimant** does not prefer **human interaction**. ★
- The **claimant** **trusts an algorithm** to be fair.
- The **claimant** values **speedy refunds**.
- The **claimant** values **transparency and clear rules**.
- The **claimant** is only **risk exposed** for a **limited time**.



PROFITABILITY

- The SM **reduces the workload** of IEX team. ★
- The claim is small but frequent.
- Few additional data or tools are required.
- A great deal of time or effort is saved.
- Reduction is not at the expense of claimants.
- The SM does not **cannibalize existing products**.
- The SM **increase sales volumes**.
- The SM **fits the current product portfolio**.
- The SM **technology can scale** to rest of portfolio.
- The SM can be sold as a B2C or B2B2C product.
- The SM has a **reasonable payback time**. ★
- The SM has a **reasonable break-even volume**.



FEASIBILITY

- We can **codify** the contract terms. ★
- We **can** define the whole **eventuality space**.
 - If not – we can create **triggers** for **manual processing**. ★
- We **can** find **reliable and willing oracles**. ★
 - There is legal support to force data sharing.
- We **can** include **breach-allowance**.
- We **can** include **contract modification or cancellation**.
- We **can** identify and eliminate **fraud loop-holes**.
- We **can** leverage existing **tech know-how**.
- We **can** **recognize if an event happens** without the claimant **having to do anything**.
 - If not – at least the claimant **doesn't have to contact us at Hedvig**.
 - If not – at least **certain horizontals or verticals** in the flow can be automated. ★

Figure 7.1: A smart contracts checklist of assumptions that need to be true in order for a smart contract to be a good fit for a claims flow. Not all statements have to hold — but for each one, the case becomes stronger. The star symbol indicates a key assumption.

Moreover, to analyse a claims flow, a generic flow chart has been developed, shown in Figure 7.2. This chart helps create a common language with regards to the different components that make up a claims flow: triggering events; questions and their corresponding data points (i.e. answers); the data points' automatability and source; the outcomes and if they involve the insurtech of study (in this case, Hedvig).

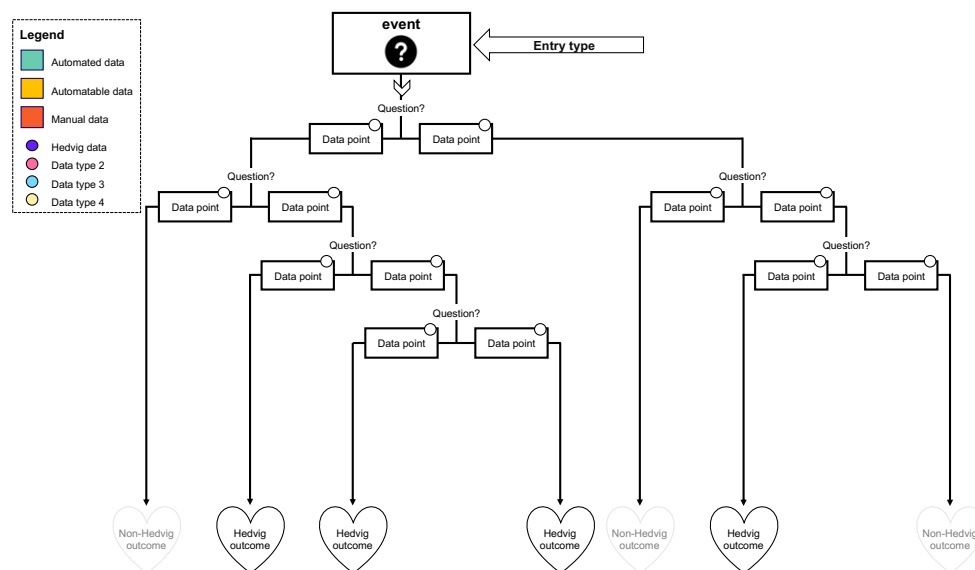


Figure 7.2: The generic claims flow chart used to illustrate Hedvig's claims.

The claims flow chart can be broken down into three types of automation: (1) data entry automation, (2) horizontal automation, and (3) vertical automation. The point in highlighting this is to recognise that full automation, while the ideal end result of a digital contract, might not be possible at the offset. However, despite this, there could be opportunities in partial automation, which could extend to a full-fledged soft smart contract in the future. Data entry automation (visualised in green in Figure 7.3) refers to when the occurrence of an event can be determined without policyholder-insurer contact.

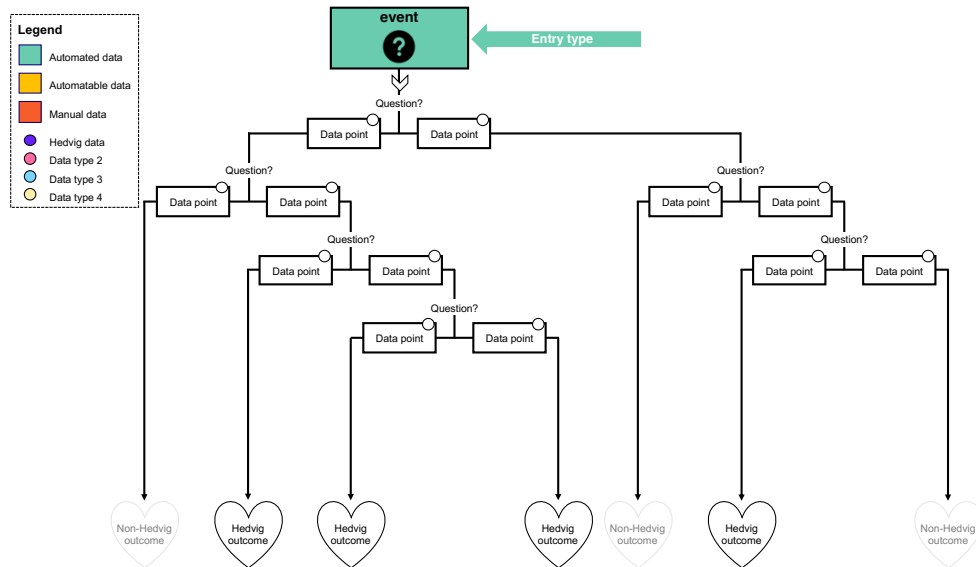


Figure 7.3: Data entry automation shown in green.

Horizontal automation (visualised in green in Figure 7.4) refers to when a certain “layer” of data (i.e. data points related to a specific question) can be fetched and answered automatically without policyholder-insurer contact.

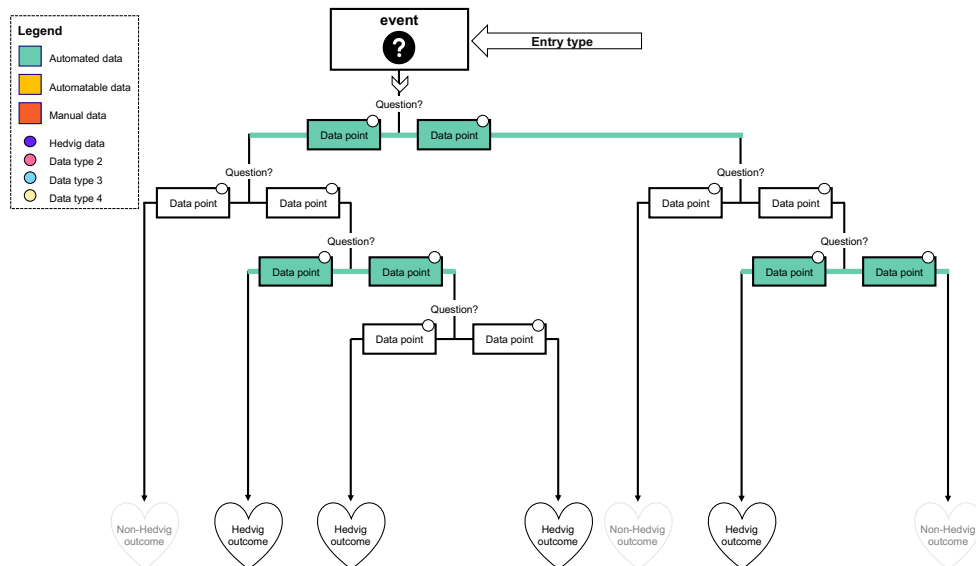


Figure 7.4: Horizontal automation shown in green.

Finally, vertical automation (visualised in green in Figure 7.5) refers to when a “path” of data (i.e. data points that a claimant has to answer to complete a claims process) can be fetched and answered automatically without policyholder-insurer contact.

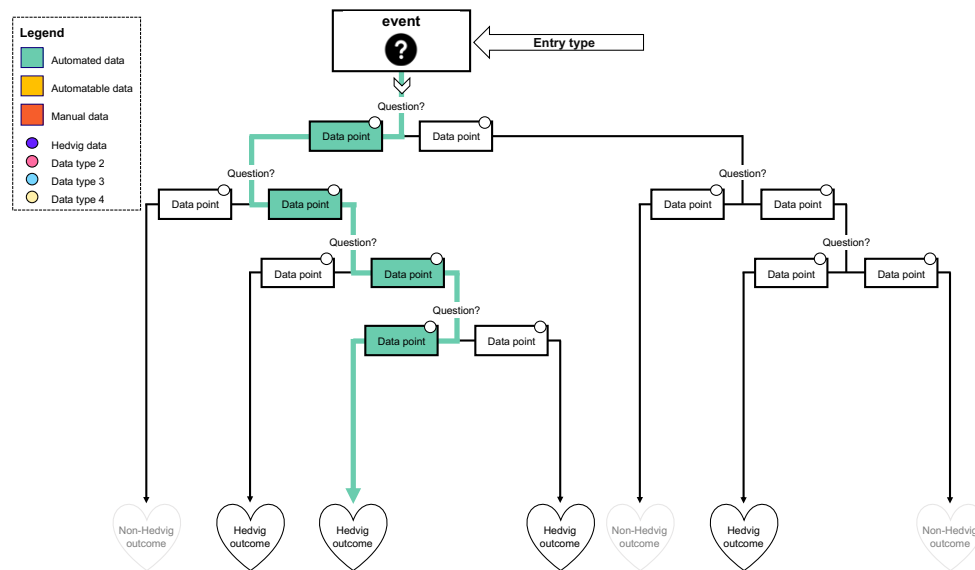


Figure 7.5: Vertical automation shown in green.

7.2 Existing Claims Flows

Three existing claims flows have been selected as units of analysis based on discussions with Hedvig’s insurance experience (IEX) team. These claims have two things in common: (1) being relatively common occurrences, and (2) taking considerable time and effort for the IEX team to complete (Jernberg, 2019).

7.2.1 Phone Damage

The phone damage claims flow is shown below in Figure 7.6.

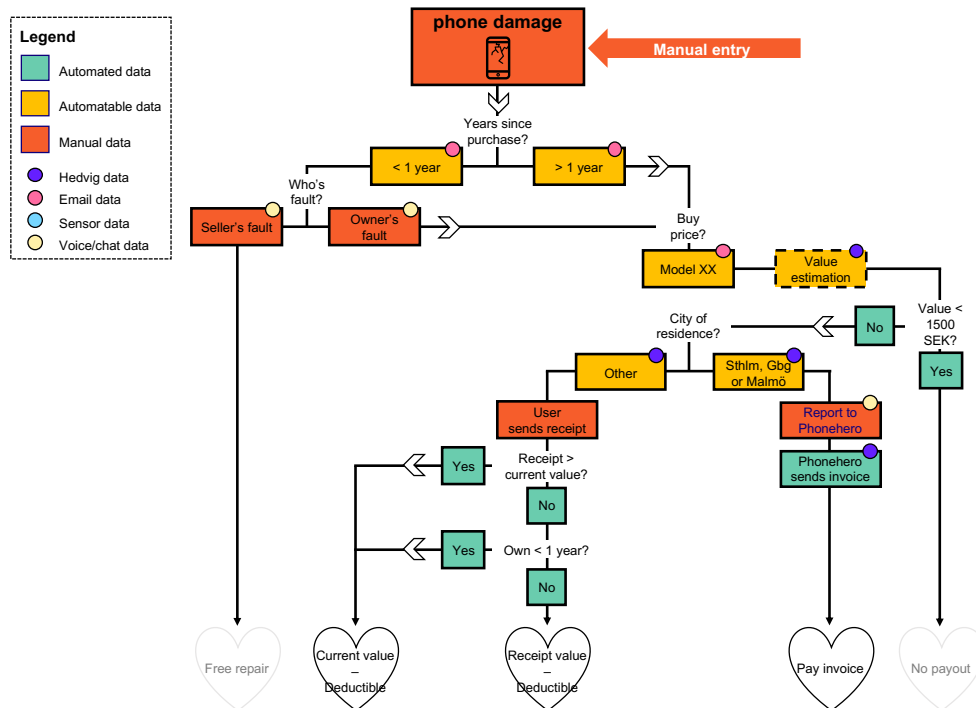


Figure 7.6: Phone repair claims flow.

7.2.1.1 User Desirability

The value proposition for users is not obvious. Some aspects of the phone damage claims flow speak for a good fit. The value calculation (i.e. how the eligibility for and amount of compensation is determined) is clear. The damage type is a relatively common occurrence and falls into a low- to medium-cost category. Also, human interaction is unlikely to be key.

However, there are some considerable shortcomings. Mainly, that this type of smart contract would not substantially improve peace of mind or convenience. As previously mentioned, the user still has to repair their unit, which requires a manual process. Moreover, this also means that the speed of the claim is limited by third-parties. Costs cannot be embedded in a smart way, and coverage cannot be extended as the market is already saturated. Finally, it does not really operate in a low-trust environment.

7.2.1.2 Business Viability

Phone damage is one of the most common claim types. It is a core aspect of the full coverage alternative in property insurance, known as *drulleförsäkring* or *allriskförsäkring* in Sweden. As such, it fits well into the existing product portfolio of Hedvig. A smart, or semi-smart, contract aimed at phone damages would not cannibalise existing revenue, but is, however, also unlikely to increase them

considerably. This is because the nature of the claim requires a repair rather than a refund, meaning that speed is limited, and some level of inconvenience is inevitable. While sales are not affected directly, it is worth pointing out that the technology necessary to enable this automation, mainly email scraping, can scale significantly and be applied to all sorts of purchases. This could, in extension, create new value that attracts new customers or increases the retention of existing ones.

Looking at the information that can be automated with email scraping, the IEX team spends a fair amount of time manually fetching and entering these data points (Nelander, 2019). Nelander (2019) explains that it is difficult to give an exact figure of how many pass through the vertically automatable path, but suggests it is not an insignificant number. Moreover, none of these automations would come at the expense of increased user inconvenience or processing time.

7.2.1.3 Technical Feasibility

The data entry is manual in this instance but could possibly be semi-automated by having certified repair shops act as the communication link (i.e. oracle). However, this presumes that a claimant knows which shops are certified or partnered with Hedvig as well as what level of reimbursement they are entitled to by Hedvig (which risks being lower than the cost of repair). Because of this, it is unlikely that the claimant could initiate this claim without any interaction with its insurer. It is worth noting that this could change in the future, for example by having more sophisticated phones that can register even superficial damages like cracked screens.

Besides some fundamental calculations, there are no horizontal or vertical levels of automation in the flow today. But many of the data points could potentially be retrieved automatically. For example, the calculations of the current value of the phone is based on when it was purchased and for how much. Using an email scraper that fetches receipt data, this information could be fed into Hedvig.

Moreover, the claimant's place of residence should be easy to determine by looking at the address where he or she lives, which is in-house (Hedvig) data. Determining which city the address is in can be accomplished by checking the postal code against an external government agency database, which would act as a reliable oracle that, additionally, there is little to no incentive to manipulate.

Doing these horizontal automations could reduce the workload for claims handlers, effectively limiting it to listening to a voice message in order to determine who is responsible for the damages and what exactly has been damaged (which is needed for the manually filled online report sent to Phonehero, a certified repair shop which Hedvig has partnered with). Moreover, these horizontal automations could also contribute to one vertical path being fully automated: the one leading to no payout.

7.2.1.4 Conclusion: Technically Possible, Value Only for IEX Team

Automation of a phone damage claims flow can only be motivated through the lens of the IEX team, which stands to lower the workload related to one of their main

claims. However, for the user, automating this information will only result in a significantly faster answer when he or she is not eligible for a payout.

7.2.2 Water Leakage

The water leakage claims flow is shown below in Figure 7.7.

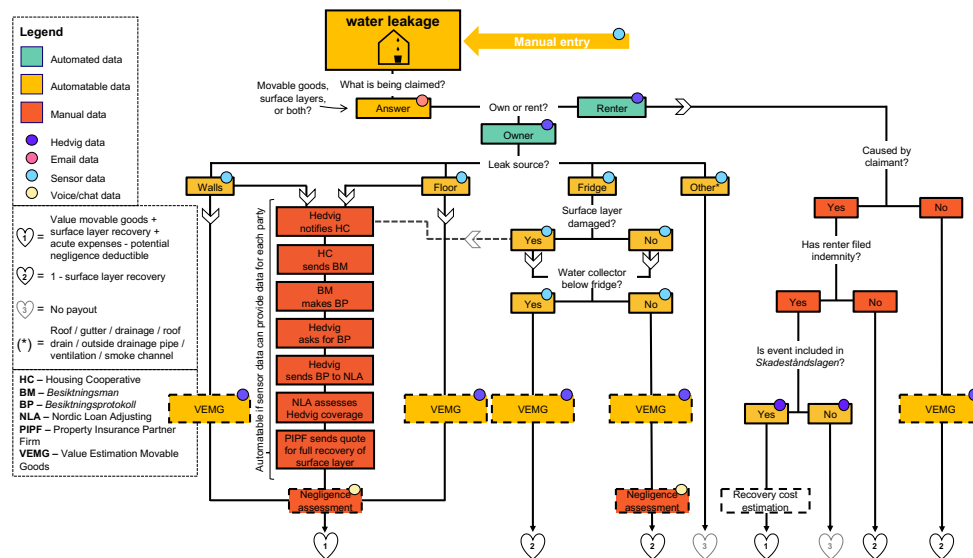


Figure 7.7: Water leakage claims flow.

7.2.2.1 User Desirability

Automation of water leakage maintenance and damage assessment, to the extent that is possible considering the third-party procedures that exist, is unlikely to create more peace of mind than is already granted. Preventive maintenance, on the other hand, has huge potential in extending peace of mind. Knowing that problems will be discovered before causing extensive damage is a powerful comfort.

Even without preventive maintenance, automation could reduce some inconvenience. It is unlikely, however, that the process of determining how much compensation should be given will be faster. Also, trust in the assessment process is probably not low, since several independent evaluators (with little incentive to be dishonest) look at the damages. It could be that increased transparency in the procedural steps of assessing the damages could be comforting and desired by homeowners.

Extensive water leakages (that would actually warrant an insurance intervention) are not very common. More importantly, when they do happen, it is possible that

homeowners would actually prefer human interaction over a computer algorithm. With high-cost damages, they might want to be comforted, listened to, or properly understood. Moreover, speedy refunds are not the key driver, but rather knowing quickly that the insurer will cover whatever repairs are necessary.

7.2.2.2 Business Viability

It is likely that an extensive sensor infrastructure would reduce the workload of the IEX team, since it would be easier to determine the nature of the damages. A lot of the data input that is today taken verbatim in an initial user statement would instead be based on actual data from the home. However, the claim is not very frequent (although more time-consuming) and would require a great deal of additional tools to be developed. The development costs associated with this sort of data collection are substantial and should not be neglected.

While the product fits well into the existing portfolio and does not cannibalise on other products, it is unlikely to increase revenue in a significant way. It is possible that a “connected home” — with extensive sensor infrastructure — is value-adding enough to increase insurance sales if it enabled proactive and preventive maintenance. That is, it would be possible to fix piping or home appliances immediately when they break down, or even before they do, and thus avoid that the water that leaks all-together.

The technology is unlikely to scale particularly well, since the sensors serve a specific purpose. However, the more sensors are connected, the more potential applications could be developed to coordinate actions that relate to triggers in or between them.

7.2.2.3 Technical Feasibility

Automation of the water leakage claims flows is a considerable technical challenge. The issue is twofold. First, it is a matter of having an extensive and reliable sensor infrastructure that can provide enough data to conclusively tell the story of the damages. Second, there are many different third-parties involved, with their own assessment procedures and ways of determining exactly how compensation should be made.

At this time, notably with limited in-depth knowledge of the procedures of the third-parties, it seems extremely difficult to automate the processes of said third-parties. One could argue that the sort of internet of things (IoT) integration that is expected to emerge in the coming years will at least enable the simpler aspects (e.g. determining the leak source, or if the surface layer is damaged) to be automated. An outcome of this could be that the third-parties actually adjust their procedures to better fit the data available, although this is only likely to happen to a limited extent.

There is also an issue of reliability, even with an extensive sensor infrastructure. What happens if a sensor fails? What is to prevent a homeowner, or another malicious or fraudulent actor, from manipulating sensor data? These are questions

that will need to be answered as the physical world continues to be integrated with the digital.

7.2.2.4 Conclusion: Technical Challenge, Value in Preventive Maintenance

The technical feasibility of a smart contract for water leakages is limited. It is possible that this will change with time and a more commonly adopted IoT infrastructure. However, coordination between third-parties greatly increases complexity.

There is some value for both IEX team and user. However, by far the greatest benefits are seen in preventive maintenance: avoiding the claims flow all-together through a soft smart contract that uses sensors as oracle data to predict breakdowns or remedy them instantly.

7.2.3 Bike Theft

The bike theft claims flow is shown below in Figure 7.8.

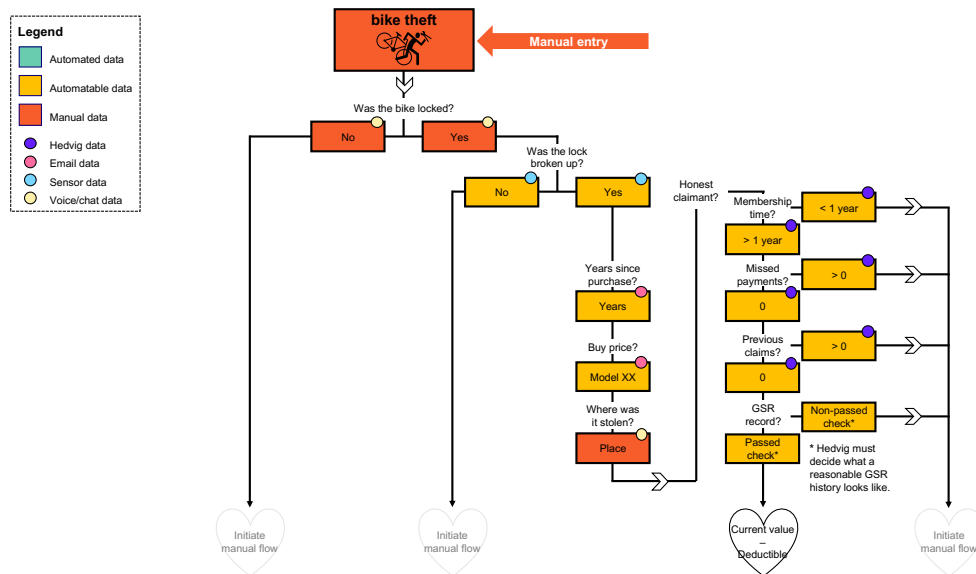


Figure 7.8: Bike theft claims flow.

7.2.3.1 User Desirability

One could argue that bike theft claims operate in a somewhat low-trust environment, since the user is unsure of what the claims handler considers to determine the claim legitimate. In the phone damage case, a certified repair shop makes an assessment that is difficult to argue with. In this sense, automation with clear-cut rules (or at

least an explanation of the use of trust indicators) might increase trust. It could, however, be a double-edged sword, causing further confusion and anger about the fairness of the indicators.

It is possible that the convenience gains are somewhat greater here than in the phone damage case, albeit marginally. Getting a payout fast (which would happen for the vertically automated path) could speed up the purchase of a new bike. However, it is unlikely that the insurance would contribute notably to overall peace of mind. Moreover, bike theft is a rarer occurrence, unless in a city with a particular bike theft problem. The market is currently saturated with this sort of insurance. Finally, human interaction is unlikely to be key, unless users place extra value on having someone listen when their case is not provable through straightforward evidence.

7.2.3.2 Business Viability

As with the damaged phone claims, the bike thefts fit well into the existing portfolio and would in no way cannibalise the current products. However, here it is also unlikely that to lead to a substantial increase in sales. The technology could potentially scale if the same trust indicators that are used to trigger manual processing in this claims flow is used for others, too.

Workload decrease for the IEX team depends on the number of users that would pass through the only vertically automated path, which relates to those users that pass the trust indicators presented above, including a “reasonability” check done through GSR, Sweden’s Joint Claims Registration Register. Based on estimates from the IEX team, these users constitute roughly 50% of the total pool of claimants for this claim type (Jernberg, 2019). Moreover, the workload saved is not at the expense of users, since they need not do any additional work through this automation.

7.2.3.3 Technical Feasibility

As with phone damages, it is difficult to determine a bike theft without receiving a notice from the claimant. Possibly, if a bike has a sensor lock, an insurer could determine if that lock has been broken. But there are many ways in which a theft could occur. If only the wheel was locked, it could be removed, leaving the lock intact.⁷ Alternatively, the whole bike could be shipped off and then demagnetised or lockpicked at an off-site.

Determining the occurrence of a bike theft is fundamentally complicated due to the lack of data. Whereas a certified repair shop can verify damages to a phone and assess the cost of repair, such an analysis is impossible when the “damaged” good

⁷ At the time of writing, Hedvig covers all bike thefts if the bike was locked, regardless of how or where it was locked. This is planned to change, so that the bike mainframe has to be locked to something for the insurance to apply.

is presumably gone. The implication is that a substantial part of the insurer's assessment has to be based on trust rather than data. Trust, simply put, becomes a proxy to evidence.

While it is simple to think of trust as a flimsy gut feeling, that is often erroneous. Many claims handlers, including those at Hedvig, develop and use implicit approaches that involve a series of trust indicators to determine the likelihood that a claim is fraudulent. In Hedvig's case, a great deal of this data is in-house. What this implies is that one vertical flow could be automated for those claimants which pass the trust indicators. It is very important to point out that a claimant that does not pass these indicators would still be eligible for a refund. The only difference is that a manual process would be initiated, just as it is done today. In fact, the flow in Figure 7.8 shows how several questions answered in a certain way lead to manual processing.

7.2.3.4 Conclusion: Technically Tricky, Potential Value for both IEX and User

There is some potential value for both user and IEX team through this flow, but it needs to be further validated through experiments prior to any extensive commitment. The issue lies in technical feasibility, more specifically the lack of oracle data. Automating trust indicators should be the focus, in order to enable the main vertical.

7.3 New Claims Flows

7.3.1 Train Delay

The train delay claims flow is shown below in Figure 7.9.

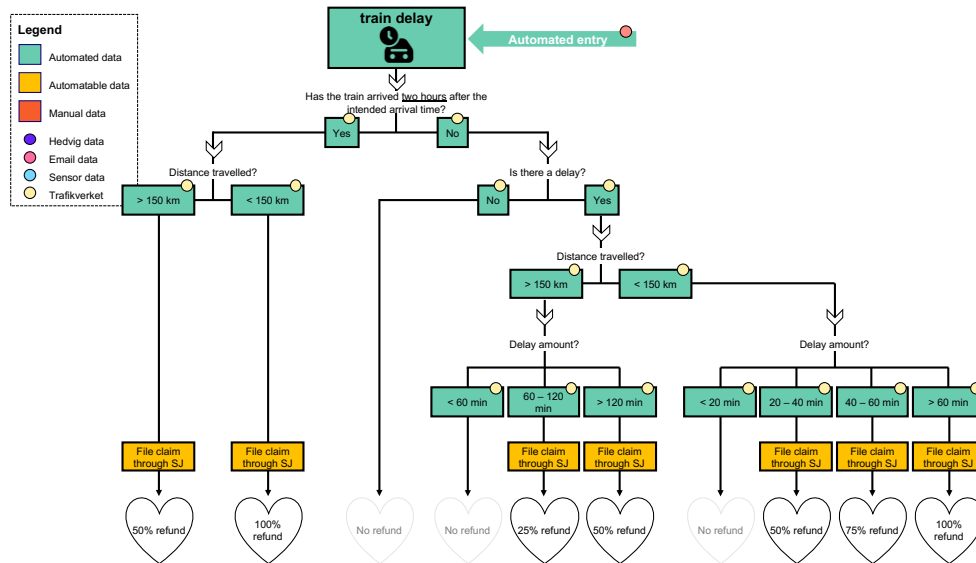


Figure 7.9: Train delay claims flow.

7.3.1.1 Technical Feasibility

This claims flow is non-existent in Hedvig's current portfolio and was developed as a proof-of-concept⁸ for the purposes of the master thesis. As such, the necessary information to build a fully automated claims flow has been gathered and validated, using a combination of Hedvig data, email scraping for ticket information, and train data from the Swedish agency Trafikverket (Swedish Transportation Administration) and the train operating company SJ (Sweden's largest train operator).

It works as follows: once a user buys a ticket from SJ, he or she receives an email confirmation and receipt. The receipt is scanned using an email scraper⁹, which collects information about the train number, departure and arrival time as well as the start and final destinations. Using a Trafikverket table on distances, the length of the trip is calculated. This is necessary as the ticket refund is based on both travel distance and delay time per SJ's refund guidelines. The trickiest part is filing a claim through SJ's claims portal. Different business models with corresponding revenue streams could be set up to enable this.

The most attractive long-term setup would be having a strategic partnership with SJ, building an integrated technology solution and applying the Hedvig brand to their claims user experience. In the short-term, a trust-based system could be set up with

⁸ This proof-of-concept is a technical schematic that can be found in Appendix A.

⁹ Such a tool has been considered for development at Hedvig.

Hedvig users to have them transfer a 10% cut in the Hedvig app, if they have been compensated by a claim that Hedvig has filed. Alternatively, this information could be retrieved by doing an additional email scrape. However, it is worth noting that having this as a free service could also serve a purpose for Hedvig; acting as a hook that attracts user to the main product.

7.3.1.2 Business Viability

Since this is a new insurance, it is of particular importance to note the effect on IEX team workload and product portfolio fit. Since it is intended to be a fully automated solution, the operational burden on the claims handling team would be non-existent; it is an infinitely scalable solution for SJ customers. Additionally, it does not cannibalise any existing product. The portfolio fit is also there. Even though it does not directly relate to home, it relates to a natural component of the everyday lives of many renters or homeowners. Hedvig also has an ambition to extend their product portfolio beyond home insurance; this is a small and simple way of experimenting in that direction.

Email scraping technology will definitely scale beyond this application (as was shown in the phone damages case). The integration into a Trafikverket API would not necessarily scale, but a strategic partnership with such an agency could act as a reference case for future partnerships. Note, however, that should the train delay smart contract be extended to other service providers, in Sweden or abroad, it needs to be redeveloped.

7.3.1.3 User Desirability

For any potential user, signing this sort of insurance would be a no-brainer limited only by one's inherent laziness or distrust as well as other superior solutions. Costs would be embedded on the condition of profit, meaning that Hedvig would not charge the user unless the user actually received a refund for delays. The user would not need to lift a finger; Hedvig would know which trips to check for and file any eventual claims. In Sweden, train operators such as SJ are not particularly well-trusted in terms of dealing fairly with claims (Dagens Media, 2015); they have a reputation of being late and designing claims flows that are inconvenient to reduce the desire to file them. Many often travel by train in Sweden, both for work and leisure. The "damages" related to delays are small to medium; not enough to warrant a great time effort, but enough to be attractive to get. Given all this, the smart contract would most likely increase peace of mind, reduce inconvenience and increase the speed of refunds.

7.3.1.4 Conclusion: Limited Direct Profit but Switching-Value Potential

The train delay smart contract is an interesting case. It is an innovative product that serves an underserved market in a way that creates clear user value without increasing the burden on claims handling teams. While the direct profit made from this sort of insurance is not huge, there is potential in leveraging the product as a

“switcher” (i.e. a product that makes a policyholder switch from one insurer to another). If this smart contract would be a standalone product, many might purchase only this to begin with, but in the long-term have a lower barrier to switch their entire home insurance to Hedvig. It is worth conducting experiments to validate this value hypothesis.

7.4 Pay-per-use Opportunities

The train delay proof-of-concept illustrates that smart contracts can be more than just a means for optimisation; they can also be an opportunity for product innovation. Further digitalising the insurance product and making it self-executing is new territory. Moreover, it is worth noting that this type of self-executing contract does not necessarily have to be directly related to claims management.

An example of this is how smart contracts could be built to modularise the insurance premium based on usage. These pay-per-use opportunities could be leveraged in situations where the customer is subject to temporary risk. Instead of having the cost of such situations be a fixed part of the insurance premium, they could be added to the customer’s insurance bill on a monthly basis, based on the customer’s risk exposure. Looking at Hedvig’s insurance product, three examples seem evident. First, travel insurance (which is today part of the home insurance premium in Sweden) could be paid for only when the policyholder travels abroad. A reliable oracle could be the customer’s GPS data. Second, expensive rented gear (e.g. skis, car) could be insured per use. The oracle in this case is much more difficult to determine; it might have to be based on what item is rented or where. Finally, online purchases from second-hand sources always incur a scam risk. Here, a pay-per-purchase insurance could be enacted as well, with oracle data based on email (or, if possible) credit card scraping.

These are just some examples that show how insurance could be segmented to produce more flexible, needs-based and personalised coverage. The result might be a lower base premium or a broader coverage as well as an increased sense of fairness in how the premium is calculated.

8 Adoption Barriers

In this chapter, empirical data is synthesised. A comparison with diffusion theory aims to determine the explanatory force of different models. Factors that drive diffusion are presented.

The models highlighted below all center on the S-curve as a plausible population distribution for diffusion. Notably, while the literature focuses on symmetrical S-curves, it is important to note that this is rarely the case in reality. S-curves are often asymmetrical, i.e. the first (last) users are slower to adopt than the last (first), leading to a long tail.

8.1 Epidemic Model

The epidemic model mainly focuses on macro drivers of diffusion by abstracting “from differences in the goals, capabilities or actions of individual members of the population” (Geroski, 2000). This allows for an analysis of (primarily information) diffusion in a “simple, tractable, non-strategic setting” (Geroski, 2000). While somewhat simplistic, it still creates a powerful framework for thought that has some degree of real-world applicability.

8.1.1 Information

The primary adoption driver in the epidemic model is information. As information diffuses about a new technology — what it does and how to use it — the adoption of it increases. On a fundamental level, the pace of adoption increases in cases where the technology is clearly superior to the old one and does not incur prohibitive switching costs. In this model, some firms finding out about a technology later than other firms partly explains their lagging behind. The same logic could be applied to entire industries, although such a scenario is more unlikely.

At face value, this seems to be a poor explanation for the lack of adoption of smart contracts in the insurance industry. Blockchain is a hyped technology that attracts a great deal of attention and investment in adjacent industries. Geroski (2000) makes note of this theoretical shortfall by pointing out that “technology

adoption often takes an order of magnitude longer than it takes for information to spread”. A better way of explaining this phenomenon would be by highlighting the “hardware” and “software” aspects of new technology. Whereas hardware is the physical (arguably also digital, although Geroski does not state so) embodiment of a technology, software refers to the information base needed to effectively use it (Geroski, 2000). In many cases, this information base can only be built through practical experience, which often implies the creation of some tacit knowledge.

And, without good software knowledge, many potential users will not adopt the new technology, however aware they are of its existence. (Geroski, 2000)

The simpler the technology — with easily learned and transmitted software knowledge — the faster the diffusion. Blockchain could be seen through this lens: a technology that everyone is aware of, but few understand how to leverage effectively. To borrow Fred Davis’s (1989) Technology Acceptance Model (TAM), which focuses on (1) the perceived usefulness and (2) the perceived ease of use of a technology, the lack of clear use cases indicate limits to the former, and the lack of infrastructure and standards limits to the latter.

It is worth recalling that two of the model’s key factors change over time. First, the total pool of potential users is not static. Improvements to a technology over time could make it viable for a segment that has previously had poor product-market fit:

Suppose, for example, that there are two groups in the population: those for whom the new technology is ideally suited, and those for whom it initially does not work as well as existing alternatives. Further, imagine that the new technology gradually improves in a way which makes it increasingly suited to the needs of the second group. (Geroski, 2000)

This could potentially be the diffusion trajectory of strict smart contract applications. It is likely that the technology will be widely adopted in financial transaction services before moving into insurance, which is more oracle-reliant. Refinements along the way would improve the technology at the same time as standards and infrastructure are being formed. As such the total pool of potential users could increase to encompass insurance.

Second, the pace of information diffusion declines over time. This could be explained by several factors: that non-users become increasingly resistant to word-of-mouth information; late adopters are less able to understand the technology; early users become less engaged in their advocacy of the technology; and so on. It is still too early to determine the extent to which this applies in the blockchain-based smart contract case, as the technology has so far barely diffused in insurance at all.

In conclusion, while the spread of information is in itself insufficient to explain the adoption of strict smart contracts, adding the TAM concepts of perceived usefulness and ease of use (which are closely related to the idea of software knowledge) help make sense of it. This explains the greater adoption of soft smart contract compared

to strict ones. Should the software knowledge requirements of blockchain-based smart contracts decrease, the pace of adoption might increase. Moreover, should such contracts find a foothold in financial transaction applications, or for that matter low-trust markets, they might eventually find their way to insurance, as the technology improves along with standards.

8.1.2 Homogeneity and Proximity

Furthermore, the pace of information diffusion can be understood by examining homogeneity and proximity. The idea is that information spreads faster when the population is densely packed and where the mixing of groups within the population comes easy (Geroski, 2000).

With the ICT revolution and the globally connected world it created, one could argue that the impact of proximity has become less evident. The internet has removed many traditional barriers of communication; the physical density of people has a smaller effect on the proliferation of information and ideas. Although it is worth noting that the internet has a tendency to generate filter bubbles and cater content that amplifies polarisation, this is more pronounced in the case of politics rather than technology news.

If groups are siloed from, or have difficulty understanding one another, word-of-mouth diffusion becomes limited. One could argue that this is the case for strict smart contracts, with groups like the blockchain community, the media that covers it, and business interests seeking to leverage it. There is a gap in understanding between the avid blockchain advocates — who seek to fundamentally upend the intermediarised structure that characterises most markets — and the rest. When the underlying philosophy behind blockchain gets lost in translation, so does an understanding of its usefulness. Businesses that want to find the next competitive edge using blockchain are in many cases missing the point. The media is also partly to blame, amplifying the hype that has hid the lack of clear use cases, or the existing use cases' lacking superiority over other solutions.

8.1.3 Profits, Learning and Risk

Finally, one could break down the technology's information into three pieces: expected profits, learning, and risk (Geroski, 2000). Any potential user considering the information at hand is looking to answer the following: What profit do I stand to make from adopting this? How much do I need to learn to use the technology efficiently? What is the risk of failing to learn, or the technology not living up to its promise?

Using this lens, it is easier to see the limitations of blockchain-based contracts. The potential profits are muddled with justified concerns about the technology's hype,

the learning curve seems daunting, and the risk of squandering investments is relatively high. For soft smart contracts, these factors are significantly lessened, although not entirely removed.

8.2 Probit Model

Probit models differ from epidemic models by focusing on micro drivers of diffusion:

It is important not to lose track of the fact that the decision to adopt is a choice made by a particular individual or (firm), and that agents frequently make different choices for the best of reasons. It follows that differences between individuals may have a potentially important role to play in explaining patterns of diffusion. (Geroski, 2000)

For example, in the above-mentioned section focusing on profits, learning and risk, the interpretation of the information was thought to be uniform across all potential users. In reality, such an interpretation differs based on the conditions of each decision-making firm.

8.2.1 Firm Size

One of the commonly observed individual traits of a firm is its size. This is “partly because it is relatively easy to observe, and partly because it is typically taken as a proxy for all kinds of things” (Geroski, 2000):

[...] large firms are sometimes thought to be more capable (they may have higher quality or more technically able people on their staff), and, for this reason, they may be less likely to need word of mouth persuasion to adopt; they may use process innovations more intensively (e.g., on a larger scale) and so earn more profits from adopting than smaller firms would; they might be less (or, for that matter, more) risk averse; they may be freer from financial constraints; they might have market power or be more inclined to strategically pre-empt smaller rivals; the new innovation might be complementary with other activities they undertake or be capable of being applied to a wider range of activities than would be the case if the adopting firm were specialised; and so on. (Geroski, 2000)

Geroski (2000) concludes that “large firms are, by and large, quicker imitators than small firms”. This is an interesting statement, especially since the article was written in 2000, well before the maturity of the internet-based startups era. In fact, in the insurance industry, the contrary seems to be true: (small) insurtechs are often the early adopters of new technology. It is possible that when highlighting that larger firms tend to have more technically competent staff, the author neglects to mention the role a massive bureaucracy (which is typical of large firms) can play in inhibiting

innovation. Large firms might also be plagued by more office politics and budgetary infighting, which counters the benefits of having better financials, bigger markets (where the technology can have impact) or being more inclined to strategically pre-empt smaller rivals.

Clearly, smaller firms in insurance have gained traction because they are filling a void the incumbents fail to address. This void is driven by digital technology and its relation to customer experience. The incumbents, rather than focusing on developing their own digital technology, have seemingly responded by artificially (and sometimes legally dubiously) raising the market barriers of entry, for example by making it more difficult for policyholders to switch their insurance through the help of competing insurance companies (Jernberg, 2019). The explanation for this may lie beyond diffusion theory. Traditional insurance companies have specialised in actuarial sciences — assessing risk by applying mathematical and statistical methods — rather than building captivating digital user experiences. The lack of absorptive capacity (Cohen & Levinthal, 1990) could explain why, then, the insurtechs (although smaller) are better able to adopt and leverage the arsenal of new technologies available and emerging:

Absorptive capacity is built up through prior experience and having related knowledge within the firm. In other words, a firm must have a certain level of existing technological knowledge in order to be able to recognize the potential of new information or technology to enhance its knowledge base. (Davenport et al., 2003)

Thus, while the probit model would suggest that bigger firms should adopt smart contract technology faster, the large insurance incumbents specialisation in narrow technologies, combined with bureaucratic governance in an increasingly fast-paced competitive landscape, might inhibit their relative ability to absorb new technology, when compared to the small insurtechs.

8.2.2 Suppliers

Another key driver is suppliers, which are “frequently responsible for facilitating the flow of information about the new technology, and, more generally, for marketing it” (Geroski, 2000). This harkens back to the epidemic model, but with a more firm-specific flair:

[The suppliers’] pricing and servicing policies have a direct bearing on the cost of new technology acquisition, and their success at designing a new technology which exactly meets the needs of the using population can often be the deciding factor between successful, rapid diffusion and outright failure. Finally, whatever technology they have designed and however they have chosen to market it, the learning process which suppliers undergo is likely to lead to a downward trajectory in prices [...]. (Geroski, 2000)

Who are the suppliers in the case of blockchain-based smart contracts? Maybe it is the competing blockchain platforms and their communities. Or the smart contract specialists that design and audit contracts through consulting services. Or the researchers trying to develop smart contracting standards and plug-and-play software programs. What is certain is that often the blockchain technology push does not come from existing suppliers but new ones. This could be a factor slowing adoption, as it forces competition between proponents of the old and new. Moreover, incremental improvements in old technology could limit the benefits of the new.

The role the above-mentioned groups play in driving adoption is ambiguous at best. Having spoken to experts representing some of these domains, particularly consulting services, it seems that there is a market pull from businesses that is far too often driven by blockchain hype rather than any concrete needs or wants. Technological expectations are clearly high but confused. Often, these experts' job becomes advising potential clients to avoid adopting blockchain solutions just for the sake of it (Fred-Ojala, 2019; Wain, 2019). In some sense, the supplier push for the technology is replaced by a supplier pushback against hype-driven market pull.

As for the blockchain platforms and communities, the advocacy is mainly directed toward making public blockchains mainstream. It is in them that the most unique and radical value resides, rather than the permissioned and private designs that are most commonly discussed for insurance applications.

Most interesting is the role of the companies trying to develop smart contract standards and plug-and-play solutions, such as Deon Digital (Henglein, 2019) or OpenLedger (Crillesen, 2019). For them, technical complexity seems to be an adoption barrier for potential users, rather than pricing or servicing. Developing an interface for the simple creation of smart contracts is therefore essential. If that is possible remains to be seen.

8.2.3 Costs

Finally, there are firm-specific costs which relate to different activities. There are learning and search costs related to the organisation's information flows as well as its risk profile (i.e. the amount of risk it is willing to tolerate). This is similar to the epidemic model, although that model implied that these were pieces of information that each and any firm would act similarly upon receiving. As mentioned, the learning curve of blockchain might be steeper than businesses desire, and the risk of failure greater than they are willing to bear. Even search is to some extent difficult, as one must constantly find the signal in the noise; that is to say, determine what is of value in the vast pool of information about the technology. Here we return to each individual firm's absorptive capacity, or their technology strategies (that is, the acquisition, management and exploitation of technology) in general.

Additionally, there are switching costs, which were also mentioned briefly before. The switching costs related to strict smart contracts have to do with legacy IT systems and architecture; the flexibility of semantic contracting, which if removed would incur considerable cost; government and regulatory unacceptance; potential cannibalisation of existing products; and, in general, organisational and business model changes as the technology opens up for new products and services. This would suggest that the adoption issues are endemic to the entire industry rather than a single firm. Organisations with deep inertia will of course have higher switching costs:

Firms that find it easier to spot costs than new sources of revenues may well be more reluctant to adopt a new technology than others. (Geroski, 2000)

Finally, there are opportunity costs. If firms have invested heavily into other technology, they might be less inclined to squander that investment. The newer the capital stock, the more reluctant to shift to new technology, given that they are incompatible.

The cost perspective is hard to delve into without deeper insight into the specific set-up of incumbent insurers and insurtechs. What is possible to gauge, and has been stated before, is that the insurtechs seem better geared toward general high-tech adoption; they spawn from the tech industry rather than insurance. In fact, only one employee at Hedvig has an insurance background (Fors, 2019). This differing nature could manifest in lower search, learning and switching costs. One could also argue that the opportunity costs are lower, as many of the insurtechs are small and recently founded.

8.3 Density Dependence Model

Population ecologists “use density dependent growth models to account for the systematic increases and decreases in net birth rates which they observe in natural settings” (Geroski, 2000). A population is thought of as having a natural rate of increase and a carrying capacity (the upper bound of the population size which can be supported). The underlying mathematical formula for these concepts is similar to that of the epidemic model, but the explanations for what drives growth is different.

8.3.1 Legitimation

The force of *legitimation* (i.e. acceptance) increases birth rates:

In the context of organizations, legitimation is the process by which a new type of organization becomes accepted, institutionalized or simply just taken for granted,

and it clearly depends amongst other things on the number of such organizations already in existence. (Geroski, 2000)

Fitting this in the context of new technology, the way to legitimation (and thus to increased adoption) comes by proving that the technology works, whether it is an improvement to the existing or other new technologies, whether there is a supply infrastructure that supports adoption, and whether there are buyers that will purchase products using the new technology (Geroski, 2000).

This legitimation process is clearly analogous to a standards setting [process], and that means that its length is likely to depend on switching costs between the old standard and the new standard, the size of the installed base of new users and expectations about market growth and the future evolution of technology. (Geroski, 2000)

This is arguably at the heart of the lacking adoption of blockchain-based smart contracts: the process of legitimation is slow. Although the expectations about the future evolution of the technology are high, the lack of (1) standards and infrastructure, (2) stakeholder adoption and government acceptance, and (3) usability and understandability, creates a climate of skepticism.

8.3.2 Competition

As a technology becomes widely adopted and established, a second force overtakes legitimation. The force of *competition* increases death rates:

Competition arises whenever resource constraints limit the number of organizations which can survive in a particular market (or social setting), and depends mainly on population density in these models. (Geroski, 2000)

In the technology context, widespread adoption “lowers the returns earned by early adopters,” meaning that it becomes less valuable to new adopters as the competition for the goods or services that use the technology increase.

However, the strategic response to competition can be more complicated than that. Since firms know that competition decreases adoption, they might be inclined to pre-emptively adopt the technology to dissuade rivals, which could actually speed up adoption in the beginning. In fact, some firms which engage in activities that the technology complements better than its rivals, will be incentivised to act first. This is called the *pre-emption effect* (Geroski, 2000). Another such effect is *rent displacement*:

Rent displacement arises when the new technology cannibalizes some of a firm's existing activities, making adoption more costly than it would be in the absence of such activities. This argument is often used to explain why incumbents can be slower to adopt new technologies than new entrants (who have nothing to cannibalize), and

it is likely to be part of any story about why market leaders who are champions of old technologies are often slower than others to adopt new competence displacing technologies. (Geroski, 2000)

In the context of smart contracts, this force may not have come into full effect yet. But it is likely that the pre-emption effect and rent displacement are driving insurtechs to adopt new technology, including smart contracts, faster than their incumbent rivals.

Another way of analysing this is that the very fact of insurtech entrance (and competition) is what will drive diffusion in the insurance industry:

There is an extensive case study literature which suggests that incumbent firms are often very slow to adopt new technologies when entry barriers are high, and this suggests that it may be that it is competition from entrants (or threats of entry) which matters most in stimulating diffusion. (Geroski, 2000)

Insurance is a conservative industry that has traditionally enjoyed high entry barriers; only recently has digitalisation created a somewhat blue ocean for consumer-facing insurtechs. It could be that history will show the role these companies play in the insurance market to be as an incumbent-modernising force, driving innovation in the industry's existing players rather than coming to dominate it themselves.

8.4 Technology Variant Model

Few diffusion models actually account for failure. But many technologies that are introduced to the market do not catch on. A way to account for this is by looking at technology variants. The idea is that, in many cases, new technologies are introduced in a variety of forms simultaneously, which spawns a variety of products (Geroski, 2000). Rarely do they all survive. How the initial choice of a technology variant is made is therefore interesting.

A fundamental factor is the idea of a *bandwagon effect*, meaning that later adopters follow the choices of early adopters. As more and more information become available of a certain variant, later adopters are less willing to consider the others. In this way, they can avoid the learning costs that the early adopters made through in their initial choice.

8.4.1 Network Externalities

The bandwagon effect is stronger in situations where *network effects* are present. If the value of a technology increases with the installed base (i.e. the number of users

that employ it), network effects exist. Network effects become even more important when the technical differences between technology variants are small (Geroski, 2000).

This is certainly the case for strict smart contracts. Consider competing blockchain platforms. They become useful the more people store information and interact on them. The technical differences are in some cases important, in others less so. For the two main platforms, Bitcoin and Ethereum, this dynamic is in full play: Bitcoin has a larger installed base, but Ethereum is more technically fit for smart contracts (Bartoletti & Pompianu, 2017). The result seems to be a difficulty of choice, which hinders the bandwagon effect of taking hold. The blockchain technologies are, in some sense, stuck in a situation where businesses are hesitant to invest in a variant, since it is still unclear which will be dominant in the years to come:

When network externalities exist, early users risk making the “wrong” choice and becoming stranded with a technology which has failed to generate the network externalities it is potentially capable of. This may make early users reluctant to move first, and may delay the adoption bandwagon. (Geroski, 2000)

8.5 Factors Driving Diffusion

Summarising these theories, one could identify a set of factors that are key determinants in the adoption of strict smart contracts in insurance. These are related to each corresponding diffusion theory model in Figure 8.1.

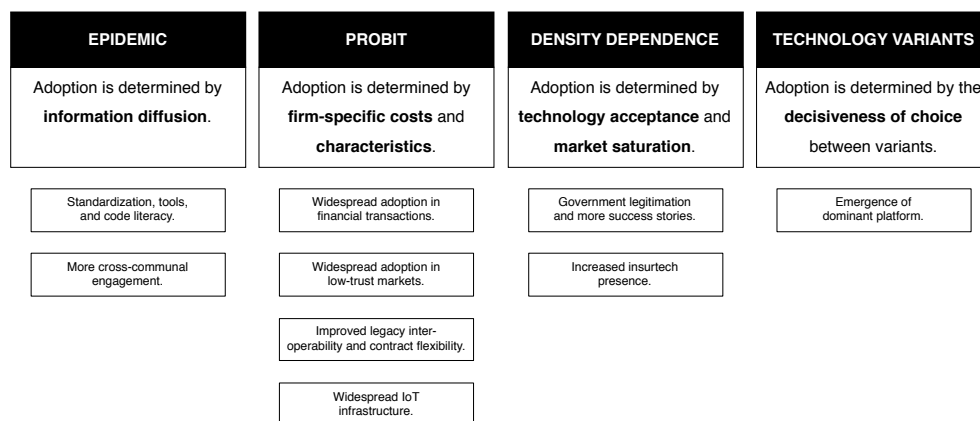


Figure 8.1: Factors driving diffusion related to its corresponding diffusion model. In this case, the probit model’s firm-specific costs and characteristics are instead considered on an industry-specific level.

8.5.1 Standardisation, tools and code literacy

High software knowledge requirements inhibit blockchain adoption. This relates to TAM concepts such as a lack of perceived usefulness and perceived ease of use, but also to code illiteracy. Not only does it decrease usage but increases the risks of poor contract design and exploitation of immutable conditions. Increased standardisation and code literacy could improve this, as would a better supporting technology infrastructure.

8.5.2 More cross-communal engagement

There is a misalignment in interest and expectation among the different communities engaged in blockchain development. While information is widespread, the heterogeneity of “senders” and “recipients” has created varied narratives and an over-hype of what blockchain can achieve. Having more cross-communal forums could ground expectations and create a common path toward further development. These forums should involve blockchain developers, business and government representatives, and legal experts, among others.

8.5.3 Widespread adoption in financial transactions

It is evident that the current fit between blockchain technologies and the insurance industry is lacking in digitally mature and institutionally democratic markets. There is a better technology-market fit in financial transaction services. As adoption picks up in that area (driven by fintech start-ups, big banks and regulatory entities alike), it is likely that the technology and its supporting infrastructure will develop incrementally to a point where adoption in insurance becomes more viable. Issues related to illegal or malicious usage, performance and scalability, privacy, and cryptocurrency volatility, which relate as much to financial transactions as insurance, would have been addressed (and possibly solved) to some extent.

8.5.4 Widespread adoption in low-trust markets

Similar to the application in financial transactions, it is likely that blockchain-based smart contracts will diffuse faster in markets that are corrupt, inaccessible or otherwise underserved by the existing institutions. Here, the full benefits of blockchain can come into play.

8.5.5 Improved legacy interoperability and contract flexibility

The switching costs for businesses interested in blockchain-based smart contracts are substantial. IT system switches or redesigns are often enormously costly and time-consuming; blockchain integration or migration is no exception. Moreover, the lack of flexibility present in semantic contracts not only creates new ex ante contracting costs but warrants reconsideration of the entire system of contracting that has grown into existence over the course of hundreds of years. Improving system interoperability would lower switching costs by allowing businesses to integrate blockchain in smaller chunks. Designing blockchain set-ups that allow for effective breach and contract modification would lower negotiation costs and bring smart contracts closer to the current legal system.

8.5.6 Widespread IoT infrastructure

The profits to be made from smart contracts rely on being able to create them in the first place. For insurance, reliance on oracles creates a severe limitation to their applicability. The continued implementation of internet of things (IoT) creates new product opportunities involving household appliances, vehicles, buried infrastructure, and locks, among other things. This could increase adoption of both strict and soft smart contracts.

8.5.7 Government legitimization and more success stories

The process of legitimization is slow. Acceptance of the technology is still low among key stakeholders. Government skepticism not only prevents many key agencies from uploading their data to blockchain platforms but creates a cloud of uncertainty and regulatory risk around any private blockchain investment. Moreover, the lack of clear (and relevant) use cases and supplier infrastructure dissuades firms from investing. Should governments take a more pro-blockchain stance in the financial market, this could change. Successful use cases would also contribute, as would a better supporting supplier infrastructure.

8.5.8 Increased insurtech presence

Insurance incumbents, with considerable knowledge investments in actuarial sciences, may lack some of the absorptive capacity needed to quickly adopt new digital technology related to the customer experience. Insurtechs, on the other hand, come from the high-tech industry. The pre-emption effect drives them to find use for new technologies faster, which may well include blockchain-based smart contracts at some point. This could not only provide more use cases but force the

industry at large (which might suffer from the risk of rent displacement) to adopt new technologies faster to remain competitive.

8.5.9 Emergence of dominating platform

The prevalence of blockchain platforms and scripting languages creates investment risk. Network effects and subtle technical differences increases the difficulty of choice. This is most aptly captured in the split between Bitcoin (with a higher installed base) and Ethereum (with better smart contract functionality). While most smart contracts reside on Ethereum, the number of contract transactions on Bitcoin is considerably higher (Bartoletti & Pompianu, 2017). Should a dominant technology variant emerge, it is likely to set off a bandwagon effect which accelerates adoption.

9 Future Scenarios

In this chapter, a discussion on the future technology strategies of insurers based on different degrees of blockchain adoption is presented, using design thinking principles in a modified Grid model. This chapter uses the accumulated empirical findings to extrapolate trends.

While a high percentage of insurers fear losing business to insurtechs (see Section 3.3), the near-term outlook suggests insurtechs will focus on the distribution side of the insurance value chain and partner with incumbents that can provide them with legal and financial support. However, widespread adoption of blockchain technologies could change the market dynamic. Hence, it is valuable to make a scenario analysis based on the degree of blockchain adoption.

Here, the aim is to build on accumulated empirical findings to extrapolate trends on how insurance companies might work with smart contracts to increase the desirability and profitability of their business as well as the feasibility of the underlying technology. The modified version of the Grid model is used for this purpose.

9.1 Scenario 1 — Minimal Blockchain Adoption

In the insurance industry, blockchain adoption is non-existent or minimal. This scenario could occur for myriad reasons. It could be that key adoption factors (see Section 8.5) are not realised. It could be that the strengths (see Section 6.1) are overestimated and the weaknesses (see Section 6.2) underestimated. It could be that new or existing technology manages to deliver some of the features that are today blockchain-specific. In any case, the result would be a significant lowering of the value in strict smart contracts.

What is likely to happen is that some of the potential value in blockchain-specific features are partially realised through soft smart contracts or other simpler technological means. Notably, these solutions would have to be implemented on the insurers' own initiative. For example, consider transparency. While public blockchain-based smart contracts would be inherently transparent, firms that see the

customer value in transparency can still strive for it through other means. In claims management, insurers could create visual interfaces for the decision trees that govern claims handling. They could enable policy modularisation, meaning that the policyholder can handpick which parts of the decision tree to have coverage for. Smart contract code could be open source and published on GitHub. All of this can be achieved without blockchain technologies.

The use of soft smart contracts would likely be as an efficiency technology, meaning that fairness is not in focus. Different insurers would compete in creating new fully or semi-automated insurance products that have previously been impossible to deliver. Existing insurance products would also be increasingly automated to relieve claims handlers and ensure business scalability. Pay-per-use solutions are likely to become more common. New revenue models might focus more on usage-based premiums, resulting in a lower base premium for the customer. More products might seek to embed costs on the condition of profit, as exemplified in the train delay proof-of-concept, in which the customer does not pay until reimbursements have been received.

Insurers attempting to implement soft smart contracts would focus intensely on finding reliable oracles, since it is arguably the biggest challenge for making them work. The value in trustworthy data would likely make them invest in improving their own databases of customer data. An example of this would be creating in-app item ledgers for their customers, which include valuables that they have purchased, in order to simplify the claims process should something break or go missing. This data might be received with the help on an email scraper. Additionally, it is likely that such insurers would partner with firms that specialise in turning semantic contracts into code, as standards continue to develop, and suppliers become more sophisticated.

But none of this would in a significant way change the underlying business model of insurance companies. The digital technology would just be a means to lower operational costs or become more user-centric. Insurtechs would still model themselves based on insurance incumbents.

Insurtechs with strong high-technology absorptive capacity are likely to have a competitive edge in terms of leveraging smart contracts, especially in the beginning. This edge, if proven to be highly desirable, could erode as incumbents augment their own capacities either through organic growth or acquisitions of one or several insurtechs. However, it is also possible that further value chain specialisation leads to insurtechs having a more permanent position next to incumbents.¹⁰ In this case, being a first-mover on building soft smart contracts could be a way to strengthen that position. By becoming experts in automating insurance operations and building

¹⁰ In Sweden, this is more unlikely than the average country, as the insurance incumbents are fullstack companies that are active in every part of the value chain.

new types of smart products, insurtechs could find new revenue either by selling insurance software or consulting incumbents. Thus, insurtechs taking the bet on soft smart contracts could create a stronger bargaining position toward both partner and competitor incumbents, allowing them to operate along a larger part of the insurance value chain.

A summary of this scenario is shown in Figure 9.1.










	DESIRABILITY	PROFITABILITY	FEASIBILITY
CUSTOMERS	WANTS & NEEDS  <ul style="list-style-type: none"> Focus on efficiency, not fairness. Partially satisfy blockchain-unique value (e.g. transparency) through simpler technologies. 	REVENUES  <ul style="list-style-type: none"> Usage-based premiums – lower base premiums or broader coverage. More products with costs embedded on the condition of profit. 	USABILITY  <ul style="list-style-type: none"> Visualise claims flows. Create interactive policies. Create item ledgers for users.
MARKET	RIVARLY  <ul style="list-style-type: none"> Insurtechs have an edge in absorptive capacity, at least initially. Insurtechs still model themselves based on incumbent business model and structure. 	BARGAINING POWER  <ul style="list-style-type: none"> Increased value chain specialisation might give insurtechs a permanent position. First-movers building soft smart contracts could benefit from consulting/partnerships. 	SUPPORTING INFRASTRUCTURE  <ul style="list-style-type: none"> Find reliable oracles. Partner with firms specialised in codifying semantic contracts.
ORGANISATION	OFFERINGS  <ul style="list-style-type: none"> Soft smart contracts in focus – no strict. Automate existing insurance products. Develop new pay-per-use products. Modularise policies to increase choice. 	COSTS  <ul style="list-style-type: none"> Scaling claims handling. Lowering operational costs. 	KNOW-HOW  <ul style="list-style-type: none"> No significant change for insurtechs. Incumbents broaden technology skillset, either organically or through acquisitions.

Figure 9.1: How insurers might interact with different technology levers to maximise the benefit of (soft) smart contracts in Scenario 1.

9.2 Scenario 2 — Widespread Blockchain Adoption

In the insurance industry, public and private blockchains are widely adopted both for consumers and corporations. Similar to the previous section, this scenario could occur for myriad reasons: the key adoption factors (see Section 8.5) are realised; the strengths (see Section 6.1) are underestimated; the weaknesses (see Section 6.2) overestimated. In any case, the result would be significant potential value in strict smart contracts.

This scenario implies a potentially radical change in terms of information availability. If one or several public or consortium blockchains become the standard repository for data, this has ripple effects for insurance. Focus would be on building strict smart contracts that both improve efficiency and ensure fairness. Oracle data becomes more accessible and reliable; the reliance on bad proxies minimised. Calculating risk premiums becomes much easier and personalised. The

transparency, security and trustworthiness of contracts is guaranteed.¹¹ The abundance of data could allow insurers to take their underwriting and fraud detection efforts to the next level. The seamless flow of data could enable radical automation of claims handling, although it is important to remember that this still relies on the codifiability of the contract. The insurers who become experts at translating policies and inquiries into binary decision points would gain a significant advantage. Moreover, the insurer will need to develop cross-functional expertise at the intersection of technology and legal domains.

As previously stated, insurtechs could have an upper hand in technology adoption, at least for a start. However, in this scenario, one could argue that the large incumbents that currently dominate the market have more influence as standard-setters. In Sweden, only a handful of incumbents account for the large majority of market share. In shaping the future of insurance with blockchain, they could leverage this dominance to build systems that are beneficial to them and poorly suited for new entrants.

More importantly, however, is that widespread blockchain adoption could force a full-scale business model transformation for insurers. Recall that in many instances, blockchain solutions eliminate the need for third-parties. As peer-to-peer (P2P) insurance solutions become globally available, this could lead to a consumer-driven push for decentralisation, which in turn could result in the complete disintermediation of the industry. The traditional role of the insurer as a trusted risk carrier could become redundant. The combination of increased consumer bargaining power and global competition paints a grim picture for traditional insurers.

The likelihood of this outcome is hard to determine and relies on many factors, perhaps most importantly the relative advantage of P2P insurance. But if this is the case, the modern insurer would have to transition from offering traditional insurance products, B2C or B2B, toward a platform-owner role that enables customised insurance, C2C. Managing a technology platform might create new revenue streams. An example could be a fee based on usage of the platform. Another would be licensing or subscription of the smart contract designs or components which are offered on it. One could argue that this sort of transition is such a massive endeavour that it is beyond the capability of incumbents, being companies with deep change inertia whose operations are heavily reliant on large centralised systems. Insurtechs might be better suited for that change, although it requires them to completely reconsider how to model their firms. While smaller and more agile, the change is still daunting. In fact, it might be other insurtechs than those in existence today that are first to rise to the challenge.

¹¹ It is worth noting that this is a miniscule issue for most current contracts in the Nordics.

If P2P is less dominating, it will still be important to standardise contract-making and focus on creating practical user interfaces for the blockchain platforms. Insurance firms will have to invest in new skillsets, particularly related to blockchain and smart contract building. New costs, for example related to smart contract auditing, increase as old costs disappear with increased product scalability.

A summary of this scenario is shown in Figure 9.2.










	DESIRABILITY	PROFITABILITY	FEASIBILITY
CUSTOMERS	WANTS & NEEDS  <ul style="list-style-type: none"> Focus on both efficiency and fairness. Potential consumer-driven push for insurance decentralisation. 	REVENUES  <ul style="list-style-type: none"> Improve risk premium calculation. Fee for usage of platform or user reach. Contract designs or components licensing or subscription model. 	USABILITY  <ul style="list-style-type: none"> Standardise contract-making. Focus on blockchain UI.
MARKET	RIVALRY  <ul style="list-style-type: none"> Insurtechs have an edge in absorptive capacity, at least initially. Existing or new insurtechs challenge the traditional insurance business model. 	BARGAINING POWER  <ul style="list-style-type: none"> Insurer as risk carrier might be redundant. Widespread disintermediation. Increased consumer bargaining power. Global competition. Incumbents use influence to set standards. 	SUPPORTING INFRASTRUCTURE  <ul style="list-style-type: none"> Huge information repository. Find reliable oracles – easier with blockchain as a data repository.
ORGANISATION	OFFERINGS  <ul style="list-style-type: none"> Strict smart contracts in focus. Possible full automation of certain policies. Enable peer-to-peer products. Build technology platform. 	COSTS  <ul style="list-style-type: none"> Less fraud – improved loss ratio. Massive organisational transformation. Smart contract auditing costs. Lower operational costs due to product scalability. 	KNOW-HOW  <ul style="list-style-type: none"> Blockchain expertise needed. Specialise in codifying contracts. Focus on technical and legal domain synthesis.

Illustration 9.2: How insurers might interact with different technology levers to maximise the benefit of (strict) smart contracts in Scenario 2.

10 Conclusions

In this chapter, conclusions and recommendations are formulated. A summary of answers to the research questions is presented. Respondent validation is connected to the thesis results. Transferability is discussed. Recommendations to the case organisation and contributions to theory are presented. A critical review of the results is discussed. Finally, suggestions for further research are given.

10.1 Answers to Research Questions

10.1.1 How can insurtechs be described and understood?

There is no agreed-upon definition of insurance technology firms, or insurtechs, but there are patterns in how insurtechs are described. Insurtechs are technology-driven companies, often startups, that take advantage of the changing technological rules and customer expectations in the insurance market.

Insurtechs belong to the ever-increasing category of firms that capture market shares in digitally under-developed industries by fusing three capabilities: (1) leveraging the most advanced technologies, (2) focusing on improving the customer experience, and (3) having an agile culture that uses advanced analytics for organisational decision-making.

By taking a position to deliver strong digital user experiences, insurtechs have seen particular success in the consumer-facing parts of the insurance value chain. They are often well-positioned to be first-movers in many new technologies, finding applications that incumbents might not have perceived due to lacking customer centricity or technology experience.

In a 2016 PwC study, 90% of insurers expressed a fear of losing business to insurtechs. But for the time being, many insurtechs are focusing on distribution rather than risk carrying; only a portion satisfy the capabilities required to be full-fledged insurance operators. This could in fact help incumbents, by creating opportunities for them to access new clients by partnering with insurtechs focusing on the customer interface.

10.1.2 How can smart contracts be described and understood?

Neither academics nor practitioners have a clear definition of smart contracts. In its simplest form, it is a digital variant of a semantic contract that automates some actions or agents in the contracting process. Take, for example, the vending machine, which automates the role of the seller based on some pre-determined terms (e.g. the price of goods, the accepted currency). A smart contract which manages to automate the role of both seller and buyer is considered self-executing. An example of this would be a flight insurance which automatically reimburses travelers for delayed flights (e.g. AXA's Fizzy).

More popularly, smart contracts are described as being blockchain-based. The reason is that blockchain enables contracting without the arbitration of third-parties. This is a radical alternative to the existing form of intermediarised market. Trust in the market, which is today guaranteed by a mutually trusted third-party, is replaced by a consensus protocol, a digital process that uses encryption and complex mathematics to create majority-rule decision-making in a network of mutually distrusting nodes. Combined with a native cryptocurrency, this enables a peer-to-peer marketplace.

This thesis project develops the following taxonomy for smart contracts, copied from Table 4.2 presented in Chapter 4.

Table 4.2: The strict and soft definitions of smart contracts.






























































































<i>Smart Contract Definition</i>	
<i>Soft smart contract</i>	Computer programs intended to digitally facilitate, verify, or enforce the search, negotiation, commitment, performance or adjudication of a contract and which can automatically move digital assets according to arbitrary pre-specified rules.
<i>Strict smart contract</i>	Soft smart contracts that can also be consistently executed by a network of mutually distrusting nodes, without the arbitration of a trusted authority.

Blockchains can be designed with varying degrees of accessibility. Public blockchains allow anyone to read data and submit transactions. The private counterparts allow only a restricted few to do so. Permissionless blockchains allow anyone to verify and process transactions (i.e. partake in the consensus protocol as a network node). The permissioned counterparts allow only a restricted few to do so. While it is the public and permissionless blockchains (e.g. Bitcoin and Ethereum

platforms) that most fully capture the unique value in blockchain, it is often a private and permissioned design that is preferred by insurance incumbents developing applications.

10.1.3 What strengths and weaknesses do smart contracts have and how does it manifest in the insurance industry?

The strengths and weaknesses of smart contracts need to be considered for both the strict and soft definition. Moreover, in the case of a blockchain-based solution, it is important to consider the degree of accessibility to the platform as well as the existence of a native cryptocurrency. What is evident, as shown in Figure 10.1, is that while the list of benefits is longer for the strict case, so is the list of drawbacks.

STRENGTHS		WEAKNESSES	
• Fast, automated and low-cost transactions	  	• "Candy" for hackers	  
• No central authority needed	  	• Oracle problem	  
• Tamper-proof	  	• Lack of flexibility	  
• No single point of failure	  	• Performance and scalability issues	  
• Full transparency	  	• Lack of infrastructure and standards	  
• Clear rules	  	• Lack of understandability and usability	  
• Huge information repository	  	• Cryptocurrency volatility	  
• Cryptocurrency integration	  	• Legal friction	  
• Global reach and access	  	• Malicious or illegal usage	  
• Equal treatment of participants	  	• Reducing users' privacy	  
• Pay-per-use insurance products	  	• Over-hyped	  
• Peer-to-peer insurance products	  	• Gov't and regulatory unacceptance	  
• Lower operational burden in claims mgmt.	  	• Lack of ecosystem stakeholder adoption	  
• Policy modularization (choice empowerment)	  	• Use of bad proxies when data is insufficient	  
• Better risk assessment and pricing	  		
• Openness of platform and market	  		
• Using future IoT infrastructure	  		






LEGEND	
	Soft smart contract features
	Strict smart contract features
	Reduced with closed, permissioned design
	Reduced without native cryptocurrency
	Applies partly even without blockchain

Figure 10.1: Detailed strength/weakness matrix for smart contracts. In addition to factors sufficiently mentioned in the literature review and through expert interviews, some additional ones have been added which the thesis authors consider to be important to mention.

In fact, some of those drawbacks (e.g. lack of flexibility, performance and scalability issues) are so severe that they arguably outweigh the added benefits (e.g. tamper-proof, no central authority needed). To avoid them, private and permissioned blockchain designs must be implemented, which in turn removes some of the unique value in blockchain. Moreover, without the native cryptocurrency that exists in some of the public platforms (e.g. Bitcoin, Ethereum), it is hard to create incentives for the consensus mechanisms to work properly.

Some examples help illustrate this. First, creating a third-party-absent environment with full transparency and global reach is indeed valuable in low-trust insurance markets, but less so in digitally mature and institutionally democratic markets (e.g. the Nordics). Second, having mathematically tamper-proof (i.e. immutable) data

records creates huge costs, stemming from the subsequent lack of flexibility (e.g. ex ante negotiation) and hacker attacks as well as performance and scalability issues (e.g. storage, computational power requirements). Third, cryptocurrency integration is limited by government and regulatory unacceptance and to some extent cryptocurrency volatility. Fourth, creating a huge blockchain-based information repository requires widespread stakeholder adoption (which is non-existent) and a promise of guaranteeing users' privacy (which is challenging). Finally, the lack of clear use cases in the insurance context speaks for itself. It points to the fact that the value in blockchain is not best utilised by intermediaries; rather, the value is in removing them.

The soft case is more promising. It delivers the essential business value of smart contracts without the fuss: enabling fast, automated and low-cost transactions through clear rules and egalitarian treatment of users. This is particularly valuable in claims handling, which stands to benefit from increased operational efficiency, more convenient user experiences, and the perceived sense of fair treatment.

The biggest drawback, as with the strict case, resides in the oracle problem, which refers to finding reliable and lasting data sources about events in the world. Other problems include hacker attacks or fraudulent practices (although bugs are more easily remedied when the contract is not immutable) and legal friction (although legal compliance is easier when an accountable third-party designs the contract). Privacy will to some extent be an issue for any digital contract solution. The lack of standards and infrastructure is a considerable problem in the short-term, but likely to decrease with time.

10.1.4 What possible and concrete smart contract applications exist for Swedish insurance firms?

The most straightforward consumer-facing application areas for smart contracts are claims management and pay-per-use/micro-insurance. By examining three of Hedvig's existing claims flows (phone damages, bike theft, and water leakage), an assessment was made regarding the desirability, profitability and feasibility of smart contracts. The results were ambiguous; full automation is difficult to achieve. However, partial automation could be considered in some cases. Three aspects of automation were considered: data entry (i.e. if the outcome of an event can be determined automatically), horizontal (i.e. if a layer of data can be automated), and vertical (i.e. if a path of data can be automated). Data entry automation is considered difficult for the existing claims flows due to lacking oracle data, meaning that pure smart contracts are unfeasible. However, horizontal automation allows some degree of work relief for both claims handlers and users. In some cases, vertical automation can create an almost fully automated claims experience for a segment of users.

If instead of optimisation, Hedvig considers opportunities for creating innovative insurance products, there are some options worthy of experimentation. A proof-of-

concept was developed for a smart contract which reimburses customers travelling with the Swedish train operator SJ if they are sufficiently delayed. This set-up, designed from scratch, qualifies as a pure smart contract. Similarly, Hedvig could consider modularising their policies by developing pay-per-use options to their insurance. For example, travel insurance could be paid for on the condition that the customer travels abroad. Renting expensive equipment could incur a one-time cost to be covered. Online purchases could be covered against scams each time a purchase is made. This might allow for a lower monthly base premium or broader coverage, which then varies depending on what risk-bearing activities the customer has engaged in. This could also increase the perceived sense of fair treatment.

10.1.5 What factors hinder adoption of blockchain-based smart contracts in the Swedish insurance market, and how can they be overcome?

The barriers for adoption can be seen through the lens of diffusion theory. Four diffusion models are considered and connected to the empirical findings in order to determine their explanatory force. The result is nine factors that help drive the diffusion of smart contracts in insurance. Factors (1) and (2) relate to the epidemic model; factors (3), (4), (5) and (6) to the probit model; factors (7) and (8) to the density dependence model; and, factor (9) to the technology variants model.

1. Standardisation, tools and code literacy: Increasing standardisation in smart contract design, improving code literacy, and developing supporting technology would counter the lack of perceived usefulness and perceived ease of use.

2. More cross-communal engagement: There is a misalignment in interest and expectation among the different communities engaged in blockchain development. Having more cross-communal forums could ground expectations and create a common path toward further development.

3. Widespread adoption in financial transactions: As adoption picks up within financial transaction services (driven by fintech start-ups, big banks and regulatory entities alike), it is likely that the technology and its supporting infrastructure will develop incrementally to a point where adoption in insurance becomes more viable.

4. Widespread adoption in low-trust markets: Similar to the application in financial transactions, it is likely that blockchain-based smart contracts will diffuse faster in markets that are corrupt, inaccessible or underserved by existing institutions.

5. Improved legacy interoperability and contract flexibility: Improving system interoperability would lower switching costs and allow businesses to integrate blockchain in smaller chunks. Designing blockchain set-ups that allow for effective breach and contract modification would lower negotiation costs and bring smart contracts closer to the current legal system.

6. Widespread IoT infrastructure: For insurance, reliance on oracles creates a severe limitation to their applicability. The continued implementation of internet of things (IoT) creates new product opportunities involving household appliances, vehicles, buried infrastructure, and locks, among other things.

7. Government legitimization and more success stories: Acceptance of the technology is still low among key stakeholders. Should governments take a more pro-blockchain stance in the financial market, this could change. Successful use cases would also help, as would a better supporting supplier infrastructure.

8. Increased insurtech presence: Higher absorptive capacity and the pre-emption effect drives insurtechs to find use for new technologies faster, which may well include blockchain-based smart contracts at some point. This could not only provide more use cases but force the industry at large to adopt new technologies faster to remain competitive.

9. Emergence of dominating platform: The prevalence of blockchain platforms and scripting languages creates investment risk. Network effects and subtle technical differences increases the difficulty of choice. Should a dominant technology variant emerge, it is likely to set off a bandwagon effect which accelerates adoption.

10.2 Respondent Validation

On November 8, the thesis authors presented some of their findings — including the smart contract checklist, claims flows, and train delay proof-of-concept — to Hedvig as part of an all-staff demo. The response was general excitement, especially with regard to the smart contract proof-of-concept. Some of the senior staff, including founders, consider this sort of concept to be in line with their overall strategic direction. Hedvig as a whole, but especially the CTO John Ardelius, saw substantial value in the smart contract checklist and claims visualisations, as tools for discussion and further development.

However, there were also some more critical voices — not aimed at the proof-of-concept specifically but product innovation more generally. These individuals urged a focus on improving the claims management system in general rather than being distracted by shiny new insurance products that do not improve the core product. The sentiment was expressed mainly by the IEX team, which is an important source of insight since they stand closest to Hedvig customers. It does, however, also colour them — they are more prone to prioritise claims optimisation over new product development. Their generally positive attitude toward claims relief through automation (where it is possible) is in line with this analysis.

Two other comments are worth highlighting with regard to the proof-of-concept. First, the CEO, Lucas Carlsén, had some thoughts on how to package this type of

offering. It could either be packaged around the problem-to-solve (e.g. train delays), or the technology it builds on (e.g. email scraper). The benefit of selling the technology could be to include several problems in one more powerful offering.

Second, there is the question of scalability, which the thesis authors have also repeatedly mentioned in conversations with Hedvig. Ardelius (CTO) was curious as to what degree of commonality there are in different train operators and their claims processes, in order to determine how well this smart contract could scale to involve other Swedish or foreign operators. The thesis authors' conclusion from a preliminary study is that scalability is limited, and that development will need to be repeated (at least aspects of it) on a case-by-case basis.

Moreover, the strength/weakness matrix was shared with both Hedvig and the experts that were interviewed for the purposes of this thesis. The response with regards to its accuracy and completeness has been positive, although it is worth noting that the number of responses have been too few to accurately depict the entire pool of experts.

The concept of developing a train delay smart contract in collaboration with Hedvig was pitched to SJ in an email conversation with two staff members responsible for partnerships. Their interest in launching automated refunds through a smart contract powered by Hedvig was deemed low. The response from SJ was that they themselves have the opportunity to automate the delay refunds but chose not to place resources on it. The reason for this was two-fold. First, because it would obviously increase their expenses. Second, because they prioritise other development projects. Even though customers might use it, SJ seemed uninterested in offering such a service through a partnership with Hedvig.

On December 16, the thesis authors presented all their findings — including the adoption barriers and future scenarios — to Hedvig as part of an all-staff final presentation. The response was in line with the first demo. Although the presentation was more technically dense and theoretical, the staff found it interesting and insightful when the authors asked for feedback.

10.3 Transferability

While the thesis's case study focused on an insurtech, its findings are not confined to that sub-genre of insurance firms. Insurtechs might have a structure or culture that make them better fit to adopt new technology, but smart contracting is not beyond the reach of incumbents. In fact, the tools developed in this thesis project, such as the smart contract checklist or the claims visualisations, could be used by any insurer. Likewise, the strength/weakness matrix applies to consumer-facing home insurance applications in the Nordics, but not any specific insurer type.

However, when it comes to industry and geography, the findings are less transferable. Repeatedly, the point has been made that low-trust markets are better fit for blockchain solutions than their high-trust counterparts. More insights of this sort could surely be gathered if a deeper analysis is made of other markets. Two types of insights would be needed to increase transferability. First, exactly which of the strengths/weaknesses or desirability/profitability assumptions apply for these markets. Second, how those factors should be re-weighted based on importance and uncertainty. A similar discussion could be had with regards to industry. For example, consider financial transaction services, which seems to be a better fit for blockchain than insurance.

With that said, both the strength/weakness matrix and the smart contract checklist are likely to already contain elements that strongly relate to other industries and geographies — but need to be further validated.

10.4 Recommendations to the Case Organisation

The following recommendations are given to Hedvig:

- **Do not adopt blockchain:** Today, blockchain is too immature — with too unclear use cases and value — to constitute a sober investment.
- **Monitor blockchain adoption indicators:** Look for the nine blockchain success factors; should any be realised, it might be worth re-evaluating the technology.
- **Monitor contract-building specialists:** Look for companies that develop technologies that translate policies into code (e.g. Deon Digital and OpenLedger).
- **Partially automate claims flows:** Focus on low-hanging fruit in automation, especially where the IEX team spends a lot of time doing manual work today.
- **Build a train delay MVP:** Test the proof-of-concept for SJ with real customers; if successful, consider other claims convenience or pay-per-use solutions.

10.5 Contribution to Theory

Several aspects of this thesis contribute to academia. First, the taxonomy on smart contracts organises the “definition jungle” found in the literature and encourages a much-needed discussion on what smart contracts are and if they need to be blockchain-reliant. Second, the literature review coupled with expert interviews creates a detailed account of the strengths and weaknesses of smart contracts (both

built on blockchain and conventional digital technologies) within the insurance context. Insurance is particularly interesting to examine due to its supposed structural fit for blockchain and similarity to financial transactions, which is the most well-diffused application area for blockchain. Third, the case study highlights the actual applicability of smart contracts for an insurer, examining both existing claims flows and potential new products. Finally, the thesis evaluates the explanatory force of popular diffusion models and conceptualises the key factors which could spur blockchain adoption in insurance.

10.6 Critical Review

The conclusions made in this study are based on data gathered through the literature review and interviews. As the (strict) smart contract is a relatively new concept with few real-world use cases, extensive research has not yet been made on the topic — especially not its applications within the insurance industry. The same goes for the emerging insurtech scene, to which research has yet to catch up. Most of the 25 papers used in the literature review were not older than five years. As such, the literature review managed to be both comprehensive and up-to-date. However, it is worth noting that more real-world applications, domain experts, and industry-specific research on smart contracts is necessary to fully validate the findings of this study.

Qualitative interviews with 17 people were conducted, of which six were insurance industry experts and 11 smart contract experts. This sample consisted of people with a variety of backgrounds, in terms of involvement in the insurance landscape and smart contract technology as well as profession and geography. One problem with the sample of interviewees is that none of them had expert knowledge of both insurance and smart contract technology. It is reasonable to assume that this is simply because there are very few people who possess expert knowledge in both of these domains. Another problem is that most smart contract or blockchain experts were practitioners (entrepreneurs, consultants or senior employees at blockchain- or smart contract-related companies). This increases the risk of having biased data, as they can be incentivised to hype the technology to benefit their own business objectives. Having more expert academics or other impartial interviewees could have reduced this risk. However, to mitigate this risk, parts of the interviews were constructed to focus on whether smart contracts actually need to be based on blockchain, and dive deeper into the implications of using or not using the technology. This was done by having open questions about how blockchain-based smart contracts differ from soft smart contracts. Furthermore, these interviews were only one part in the triangulation approach used when collecting a relevant dataset, and therefore complementary to data from academic papers.

In conclusion, the results and conclusions are based on data that represent the whole population of experts within smart contracts and Swedish insurance fairly well.

10.7 Suggestions for Further Research

The research gaps — intentionally beyond the thesis project scope — are well-suited as areas for further research. First, it would be interesting to more deeply explore the insurance market pull for smart contracts or automation in general. To what extent do the customer values hypothesised in this thesis hold true as key aspects of smart contract desirability? How substantial are the risks related to privacy or integrity online? What about algorithmic bias in decision-making? Do insurance customers consider those risks prohibitive?

Second, it would be valuable to examine the non-consumer-facing aspects of insurance as application areas for smart contracts. In fact, this thesis suggests that the adoption of smart contracts is likely to occur as internal processes or B2B before B2C. Which adoption barriers apply in this context? Are the strengths and weaknesses of blockchain the same? Similarly, one could rescope the study to cover insurance types other than property and casualty insurance, or other geographies.

Third, this thesis's data naturally relies heavily on academic and practitioner knowledge of blockchain-based smart contracts, since the soft definition is introduced here for the first time. This means that the authors' understanding of soft smart contracts emerges from a focus on strict smart contracts. To further develop knowledge about the business potential in soft smart contracts, an entire study could be dedicated to mapping existing companies that use them as part of their business model.

Finally, it would be interesting to monitor the continued development of the competitive dynamic between insurance incumbents and insurtechs. How does it affect technology infusion and innovation activities in an otherwise conservative industry? Can the insurtechs create a permanent position within the insurance value chain?

10.8 Final Remarks

Insurtechs have without doubt catalysed digitalisation within the insurance industry. With an increased focus on leveraging advanced technology and creating convenient customer experiences, they have captured market shares stretching from modest to considerable. However, for the time being, it would seem that strict smart contracts will play a miniscule role in this change. Soft smart contracts, on the other hand,

have shown some promise as a means to increase operational efficiency and improve the value proposition.

In the introduction, three general risks in digitalisation were highlighted: algorithmic bias in decision-making, lack of transparency, and privacy infringement. While smart contracts (especially strict ones) could be used to increase transparency, there is still a major issue in oracle data as a source of algorithmic bias. Improper oracles, or proxies used when oracle data is non-existent, could systemise unfair or immoral decision-making on a global scale. Having full transparency could mitigate this risk, since it increases auditability. But it is a risk, nonetheless. As for privacy, one could argue that it is a rampant problem that should be addressed on a scale far beyond that of any single technology or concept.

Finally, there is the matter of practical applicability. To some extent, this thesis has shown how overhype of a general-purpose technology can confuse what concrete value it produces in a specific context. This is the case for strict smart contracts based on blockchain. But unexpectedly, the thesis has also highlighted the difficulty of examining a concept that does not have a broadly accepted definition. Soft smart contracts, while widely applied and successful in real business settings, are rarely covered in the literature. It goes to show the power of narrative in deciding the focus of subject matter discourse.

References

- Alharby, M., & van Moorsel, A. (2017). Blockchain-based smart contracts: A systematic mapping study, *arXiv preprint arXiv:1710.06372*.
- Anderson, N., Chishti, S., Millie, S. & Vanderlinden, S. (2018). *The InsurTech Book — The Insurance Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries*. West Sussex, United Kingdom: John Wiley & Sons Ltd.
- Association of British Insurers. (2019). *How insurance works*. [online] Available at: <https://www.abi.org.uk/data-and-resources/tools-and-resources/how-insurance-works/> [Accessed 15-09-2019].
- Banton, C. (2019). *Reinsurance*. Investopedia. [online] Available at: <https://www.investopedia.com/ask/answers/08/reinsurance.asp> [Accessed 20-09-2019].
- Bartlett, J. (2018). *The People Vs Tech (1st ed.)*. Penguin Random House.
- Bartoletti, M., & Pompianu, L. (2017). An empirical analysis of smart contracts: platforms, applications, and design patterns, *International conference on financial cryptography and data security*, 494-509.
- Baukloh, R., Blake, M., Evans, S. & Short, E. (2015). *Tapping into Insurance FinTech: Own it, Lease it or Share it?*. KPMG. [online] Available at <https://assets.kpmg/content/dam/kpmg/pdf/2015/07/tapping-into-insurance-fintech-fs.pdf> [Accessed 25-09-2019].
- Blockgeeks (2017). *Blockchain Glossary: From A-Z*. [online] Available at: <https://blockgeeks.com/guides/blockchain-glossary-from-a-z/> [Accessed 01-12-2019]
- Braun, A. & Schreiber, F. (2017). *The Current InsurTech Landscape: Business Models and Disruptive Potential*. St. Gallen, Switzerland: University of Saint Gallen.
- Brown, T. (2008). Design thinking, *Harvard business review*, 86(6), 84.
- Buterin, V. (2014). A next-generation smart contract and decentralized application platform, *white paper*, 3, 37.

- Caplinger, D. (2017). *Reinsurance Companies: What You Need to Know*. The Motley Fool. [online] Available at: <https://www.fool.com/investing/2017/06/14/reinsurance-companies-what-you-need-to-know.aspx> [Accessed at 20-09-2019].
- Christidis, K. & Devetsikiotis, M. (2016). Blockchain and Smart Contracts for the Internet of Things, *IEEE Access*, 4, 2292-2303.
- Chohan, U. W. (2017). Cryptocurrencies: A Brief Thematic Overview, *Notes on the 21st Century*.
- Cohen, W. and Levinthal, D. (1990). Absorptive capacity: a new perspective on learning and innovation, *Administrative Science Quarterly*, 35, 128–152.
- Cuccuru, P. (2017). Beyond bitcoin: an early overview on smart contracts, *International Journal of Law and Information Technology*, 25(3), 179-195.
- Cusano, J. (2016). *Insurtech Boom Will Reshape the Global Insurance Market*. Accenture. [online] Available at: <https://insuranceblog.accenture.com/insurtech-boom-will-reshape-global-insurance-market> [Accessed 17-09-2019].
- Davenport, S., Campbell-Hunt, C., & Solomon, J. (2003). The dynamics of technology strategy: an exploratory study, *R&D Management*, 33(5), 481-499.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS quarterly*, 319-340.
- Denscombe, M. (2017). *The Good Research Guide — For small-scale social research projects (6th ed.)*. London, England: Open University Press.
- Dickinson, B. (2015). *Insurance Is The Next Frontier for Fintech*. TechCrunch. [online] Available at: <https://techcrunch.com/2015/08/05/insurance-is-the-next-frontier-for-fintech/> [Accessed 17-09-2019].
- Eling, M. & Lehmann, M. (2018). The Impact of Digitalization on the Insurance Value Chain and the Insurability of Risks, *The Geneva Papers*, 43, 359-396.
- Etherisc (2019). *Products*. [online] Available at: <https://etherisc.com/products> [Accessed 02-12-2019].
- Fairfield, J. A. (2014). Smart contracts, Bitcoin bots, and consumer protection, *Wash. & Lee L. Rev. Online*, 71, 51.
- Fell, G. (2017). *The 4 Insurtech Blockchain Disruptors To Know*. Foresight Factory [online] Available at: <https://www.foresightfactory.co/2017/06/15/4-insurtech-blockchain-disruptors-know/> [Accessed 02-12-2019].
- Garzik, J. (2015). Public versus private blockchains. *BitFury Group, San Francisco, USA, White Paper, 1*.

- Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018a). Blockchain and smart contracts for insurance: Is the technology mature enough?, *Future Internet*, 10(2), 20.
- Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018b). To blockchain or not to blockchain: That is the question, *IT Professional*, 20(2), 62-74.
- Geroski, P. A. (2000). Models of technology diffusion, *Research policy*, 29(4-5), 603-625.
- Halaburda, H. (2018). Blockchain revolution without the blockchain, *Bank of Canada Staff Analytical Note*, 5.
- Hans, R., Zuber, H., Rizk, A., & Steinmetz, R. (2017). *Blockchain and Smart Contracts: Disruptive Technologies for the Insurance Market*.
- HarperCollins. (2019). *Definition of 'primary insurer'*. [online] Available at: <https://www.collinsdictionary.com/dictionary/english/primary-insurer> [Accessed 20-09-2019].
- Hayes, A. (2019). *Insurance Claim*. Investopedia. [online] Available at: https://www.investopedia.com/terms/i/insurance_claim.asp [Accessed 15-09-2019].
- Hedvig. (2019). *Nice Insurance to the Masses*. [online] Available at: <https://www.hedvig.com/blog/nice-insurance-to-the-masses> [Accessed 01-10-2019]
- Hu, Y., Liyanage, M., Mansoor, A., Thilakarathna, K., Jourjon, G., Seneviratne, A., & Ylianttila, M. (2018). Blockchain-based Smart Contracts - Applications and Challenges, *arXiv preprint arXiv:1810.04699*.
- Höst, M., Regnell, B. & Runeson, P. (2006). *Att genomföra examensarbete (6th ed.)*. Lund, Sweden: Studentlitteratur AB.
- Insurance Sweden. (2019). *Insurance in Sweden 2019*. [online] Available at: <https://www.svenskforsakring.se/globalassets/engelska/statistics/insurance-in-sweden-2019.pdf> [Accessed at 27-09-2019]
- Jiang, K. (2017). "Den svenska försäkringsmarknaden är inte gynnsam för insurtech". Sak och Liv. [online] Available at: <https://sakochliv.se/2017/09/18/den-svenska-forsakringsmarknaden-ar-inte-gynnsam-for-insurtech/> [Accessed 01-10-2019]
- Junis, F., Prasetya, F. M. W., Lubay, F. I., & Sari, A. K. (2019). A Revisit on Blockchain-based Smart Contract Technology, *arXiv preprint arXiv:1907.09199*.

- Kagan, J. (2019). *Insurance Premium*. [online] Available at: <https://www.investopedia.com/terms/i/insurance-premium.asp> [Accessed 01-12-2019]
- Krawiec, R., Housman, D., White, M., Filipova, M., Quarre, F., Bar, D., Nesbitt, A., Fedosova, K., Killmeyer, J., Israel, A. & Tsai, L. (2016). *Blockchain: Opportunities for Health Care*. [Online] Available at: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-health-care.pdf> [Accessed 01-12-2019]
- Lewis, S. (2017). Insurtech: An Industry Ripe for Disruption, *Georgetown Law Technology Review*, 491.
- Lexico (2019). *Definition of proxy in English*. [online] Available at: <https://www.lexico.com/en/definition/proxy> [Accessed 01-12-2019]
- Lindberg, R. (2015). *Lågt förtroende för SJ*. Dagens Media. [online] Available at: <https://www.dagensmedia.se/marknadsforing/kampanjer/lagt-fortroende-for-sj-6142615> [Accessed 02-12-2019].
- Lunden, I. (2019). *Sweden's Hedvig raises \$10.4M led by Obvious Ventures to build 'nice insurance'*. TechCrunch. [online] Available at: <https://techcrunch.com/2019/08/27/swedens-hedvig-raises-10-4m-led-by-obvious-ventures-to-build-nice-insurance/> [Accessed 01-10-2019]
- Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter, *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 254-269.
- Methodical (2019). *Meet the Grid*. [online] Available at: <https://www.methodical.io/meet-the-grid/> [Accessed 02-12-2019].
- McKinsey & Company. 2019. *2019 global insurance trends and forecasts*. [online] Available at: <https://www.mckinsey.com/industries/financial-services/our-insights/2019-global-insurance-trends-and-forecasts> [Accessed 17-09-2019].
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*.
- Nam, S. (2018). How Much Are Insurance Consumers Willing to Pay for Blockchain and Smart Contracts? A Contingent Valuation Study, *Sustainability*, 10(11), 4332.
- Nicoletti, B. (2017). *The Future of FinTech*. Rome, Italy: Springer Nature.
- Norman, D. (1988). *The Design of Everyday Things (1st ed.)*. Basic Books.
- O'Hara, K. (2017). Smart contracts — dumb idea, *IEEE Internet Computing*, 21(2), 97-101.
- O'Neil, C. (2016). *Weapons of Math Destruction (1st ed.)*. Crown.

- Oliver Wyman. (2016). *Zukunft von InsurTech in Deutschland*. [online] Available at: https://www.oliverwyman.de/content/dam/oliver-wyman/europe/germany/de/insights/publications/2016/jul/Oliver_Wyman_Policen%20Direkt_Insurtech-Radar.pdf [Accessed 27-09-2019]
- Outreville, F. (1998). *Theory and Practice of Insurance (1st ed.)*. New York, United States: Kluwer Academic Publisher.
- Pawliw, B. & Richards, K. (2018). *Definition: Cryptography*. [online] Available at: <https://searchsecurity.techtarget.com/definition/cryptography> [Accessed 1/12-2019]
- Puertas, A., O'Driscoll, C. Krusberg, M., Gromek, M., Popovics, P., Teigland, R., Siri, S. & Sundberg, T. (2017). *The Next Wave of FinTech — Redefining Financial Services Through Technology*. [online] Available at: <https://www.hhs.se/contentassets/615a9c5cac064280877d07799d70e0d2/insurtechreportssel.01.pdf> [Accessed 30-09-2019]
- PWC. (2016). *90% of insurers fear they will lose business to a start-up as investment in 'InsurTech' increases fivefold*. [online] Available at: https://pwc.blogs.com/press_room/2016/06/90-of-insurers-fear-they-will-lose-business-to-a-start-up-as-investment-in-insurtech-increases-fivef.html [Accessed 26-09-2019]
- Raikwar, M., Mazumdar, S., Ruj, S., Gupta, S. S., Chattopadhyay, A., & Lam, K. Y. (2018). A blockchain framework for insurance processes, *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 1-4.
- Raskin, M. (2016). *The law and legality of smart contracts*.
- Ricciardi, V. (2017). 'InsurTech Definition as Its Own Manifesto', Anderson, N., Chishti, S., Millie, S. & Vanderlinden, S. (2018). *The InsurTech Book — The Insurance Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries*. West Sussex, United Kingdom: John Wiley & Sons Ltd, pp. 6-8.
- Rogers, E. (1983). *Diffusion of Innovations (3rd ed.)*. New York, United States: A Division of Macmillan Publishing Co.
- Savelyev, A. (2017). Contract law 2.0: Smart'contracts as the beginning of the end of classic contract law, *Information & Communications Technology Law*, 26(2), 116-134.
- Schreiber, D. (2017). *Lemonade Sets a New World Record*. Lemonade. [online] Available at: <https://www.lemonade.com/blog/lemonade-sets-new-world-record/> [Accessed 02-12-2019].
- Shelkovnikov, A. (2016). *Blockchain applications in insurance*. Deloitte. [online] Available at:

<https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-deloitte-blockchain-app-in-insurance.pdf>

- Shrier, D., Sharma, D., and Pentland, A. (2016). *Blockchain & Financial Services: The Fifth Horizon of Networked Innovation*.
- Sklaroff, J. M. (2017). Smart contracts and the cost of inflexibility, *U. Pa. L. Rev.*, 166, 263.
- Skog, A., Lewan, M., Karlström, M., Morgulis-Yakushev, S., Lu, Y. & Teigland, R. (2016). *Chasing the Tale of the Unicorn — A study of Sweden's Misty meadows*. [online] Available at: <https://internetstiftelsen.se/app/uploads/2019/01/Chasing-the-Tale-of-the-Unicorn-A-study-of-Stockholms-misty-meadows.pdf> [Accessed 01-10-2019]
- Statista (2017). *Insurtech*. [online] Available at: <https://www.statista.com/study/46031/insurtech/> [Accessed 01-10-2019]
- Szabo, N. (1997). Formalizing and securing relationships on public networks, *First Monday*, 2(9).
- The Zebra (2019). *What is Property and Casualty Insurance?*. Available at: <https://www.thezebra.com/insurance-guide/property-and-casualty-insurance/> [Accessed 01-12-2019]
- Timmermans, S. & Tavory, I. (2012). Theory Construction in Qualitative Research: From Grounded Theory to Abductive Analysis, *Sociological Theory*, 30(3), 167-186.
- Tunstall, S. (2017). 'Why Insurance is Failing', Anderson, N., Chishti, S., Millie, S., Vanderlinden, S. (2018). *The InsurTech Book — The Insurance Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries*. West Sussex, United Kingdom: John Wiley & Sons Ltd, pp. 9-12.
- Wang, J., Wang, Q., Zhou, N. & Chi, Y. (2017). A Novel Electricity Transaction Mode of Microgrids Based on Blockchain and Continuous Double Auction. [online] Available at: https://www.researchgate.net/figure/Blockchain-structure_fig2_321322377 [Accessed 02-12-2019].
- Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., & Wang, F. Y. (2018). An overview of smart contract: architecture, applications, and future trends, *2018 IEEE Intelligent Vehicles Symposium (IV)*, 108-113.
- Watkinson, M. (2017). *The Grid (2nd ed.)*. Cornerstone Digital.
- Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger, *Ethereum Project Yellow Paper*.

- Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C. & Rimba, P. (2016). *A Taxonomy of Blockchain-Based Systems for Architecture Design*. Sydney, Australia: CSIRO
- Yuan, M. (2017). "I accidentally killed it" (and evaporated \$300 million). CyberMiles, Medium. [online] Available at: <https://medium.com/cybermiles/i-accidentally-killed-it-and-evaporated-300-million-6b975dc1f76b> [Accessed 02-12-2019].

Appendix A Proof of Concept for Train Delay Smart Contract

The proof-of-concept illustrated in Figure A.1 demonstrates a schematic of the interacting components for this soft smart contract and its high-level technical set-up.

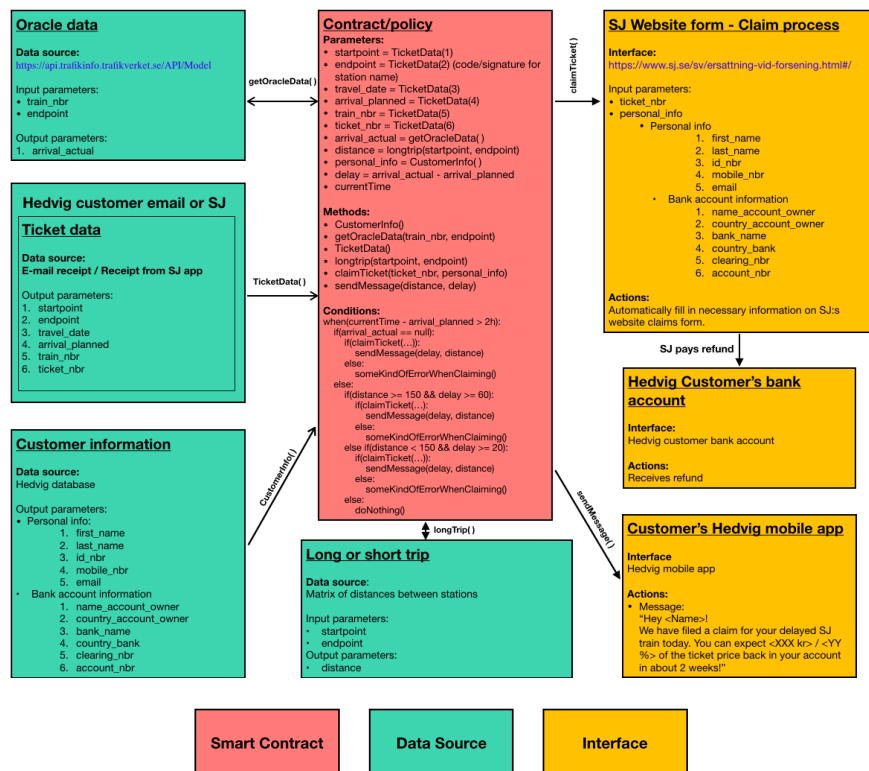


Figure A.1 - Soft smart contract schematic for SJ train delays.

The smart contract (the Contract/policy box) contains a set of code (Conditions) with the conditional statements that replicate the terms of SJ's delay policy. The conditions state what the contract should do in all the different situations. The

contract execution is based on the values of the different parameters (Parameters) in the contract, which are the data fetched from the train ticket (the Ticket data box) and Hedvig personal information (the Customer information box) as well as Trafikverket's API (the Oracle data box) and its distance matrix (the Long or short trip box). In order to assign values to the parameters and do actions such as filing the claim and notifying the Hedvig customer of a refund, a set of methods (Methods) are also defined in the contract. These methods either fetch and assign values to the parameters or perform actions on SJ's website (the Claims process box) and Hedvig's mobile app (the Customer's Hedvig mobile app box).

Table A.1 explains what the different boxes represent in the schematic, and the parameter outputs from the data source boxes. Table A.2 explains what the methods in the smart contracts do.

Table A.1: Schematic boxes and their parameter outputs.

<i>Name (Type)</i>	<i>Description</i>
<i>Oracle Data</i> <i>(Data source)</i>	<p>Trafikverket's API, which is an open data source with real-time traffic information. This data source provides the smart contract with delay information, which determines whether a customer is entitled to a refund or not.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • arrival_actual = the actual arrival time of a specific train to the train station.
<i>Ticket Data</i> <i>(Data source)</i>	<p>The digital ticket or receipt that an SJ customer receives when purchasing a ticket, which includes information about the train route. The ticket data is retrieved by the email scraper.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • startpoint = starting point on the ticket. • endpoint = end point on the ticket. • travel_date = travel date. • arrival_planned = the planned arrival time of a specific train to the train station. • train_nbr = the train number which is unique for each trip. • ticket_nbr = the ticket number which is unique for each ticket.

Customer Information
(Data source)

Hedvig's internal registry of customers and their personal information. This includes the information that is needed to file a claim on SJ's website.

Parameters:

- first_name = first name of the customer.
- last_name = last name of the customer.
- Id_nbr = ID number of the customer.
- mobile_nbr = mobile phone number of the customer.
- email = email of the customer.
- name_account_owner = name of bank account owner (first and last name of the customer).
- country_account_owner = nationality of the customer.
- bank_name = bank name of the customer.
- country_bank = country of the bank.
- clearing_nbr = clearing number.
- account_nbr = bank account number.

Long or Short Trip
(Data source)

An Excel file with a matrix with distances between Swedish train stations.

Parameters:

- distance = distance between two specific train stations.

Contract/Policy
(Smart contract)

The soft smart contract, which is the code that automatically executes under certain predetermined conditions and has defined outcomes based on SJ:s refund guidelines, as well as coded methods for submitting a claim to SJ and notifying the Hedvig customer.

SJ Website's Claims Process
(Interface)

The website form where the smart contract submits a delay claim to SJ. Uses the ticket number and customer information that is necessary to fill out the form.

Hedvig User's Bank Account
(Interface)

The Hedvig customer's bank account where SJ sends the refund.

Hedvig User's Mobile App

The Hedvig mobile app of the customer, to which the smart contract sends out a notification about the made claim.

(Interface)

Table A.2: The smart contract methods.

<i>Name</i>	<i>Description</i>
<i>getOracleData()</i>	Fetches the actual arrival time of a train from Trafikverket's API, using its train number and trip end point as input parameters.
<i>TicketData()</i>	Sends relevant ticket data to the smart contract. The data is scraped from the customer's train ticket on their email.
<i>CustomerInfo()</i>	Sends the customer's personal information and bank account information from Hedvig's internal database to the smart contract.
<i>longTrip()</i>	Fetches the distance of the trip from the distance matrix, using the specified starting point and end point in the ticket.
<i>claimTicket()</i>	A method that enters the SJ website's claims form and submits the ticket number and customer information.
<i>sendMessage()</i>	A method that sends a notification to the Hedvig customer's mobile app, where the message content depends on delay time and distance of trip.

Appendix B Interview Guides

B.1 For Smart Contract and Blockchain Experts — Round 1

- Tell us about your background and how you have worked with smart contracts (and insurance industry if applicable)?
- How do you define smart contracts?
- What is your general opinion of smart contracts: potential, applicability, urgency?
- Can you give us some examples of real use cases?
- Within which application areas are smart contracts most promising?
- What strengths and weaknesses do you see in the technology?
- How far away are smart contracts from mainstream adoption? What roadblocks have to be overcome?
- What is needed, from a practical standpoint, to set up a smart contract? Besides writing the codified contract and connecting with appropriate oracles?
- What do you need to consider/think of when designing and implementing smart contracts?
- Is it necessary to build smart contracts on blockchains?
 - Can you capture the same business value without blockchain?
- Is it generally difficult or easy to find and connect with relevant oracles?
- How are security issues dealt with relate to oracles?
- What do you consider the key application areas of smart contracts in insurance?

B.2 For Smart Contract and Blockchain Experts — Round 2

- Tell us a little bit about your background and how you have worked with smart contracts?

- What would you consider the strengths and weaknesses of smart contracts, specifically in the insurance industry?
 - If not done already: Please specify how and why the strengths benefit the insurance industry.
 - Can the weaknesses be managed/solved? If yes, how?
- What are the most value-adding applications of smart contracts in the consumer-facing parts of insurance?
 - Why are these applications the most value-adding ones?
- Does a smart contract have to be built on a blockchain?
 - If so, what are the main differences of blockchain based smart contracts?
 - What would be the value for of smart contracts not built on blockchain, in an insurance context?

B.3 For Insurance Industry Experts

- Tell us a little bit about your background and how you have worked with the insurance industry.
- Who do you consider to be the main actors in the traditional insurance ecosystem?
- How do you define insurtechs?
 - What makes them different from traditional insurance companies?
- How has the emergence of insurtech affected the traditional insurance industry?
- How would you describe the insurance value chain?
 - Which parts of the insurance value chain are most relevant for insurtechs?
- Are there any insurance companies or insurtechs who use smart contracts today, that you know of?