The Minimum Hybrid Contract (MHC): Combining Legal and Blockchain Smart Contracts

Master Thesis

Jørgen Svennevik Notland

Norwegian University of Science and Technology (NTNU)

School of Entrepreneurship

TIØ4530

Spring 2019

Faculty of Economics Management

Department of Industrial Economics and Technology Management.

Supervisors: Roger Sørheim & Donn Morrison

NTNU SCHOOL *of* ENTREPRENEURSHIP

Table of Contents

Abstract

Having identified contracts as the nexus of corruption, I sought to find how contacts, blockchain smart contracts, and financial regulations can be used to make them both secure, accountable, transparent, and inclusive. Then I explored how corruption in a contractual relationship could be mitigated, using the term Minimum Hybrid Contract (MHC) which I coined, where a smart contract is a supplement to a legal contract providing transparency and immutability to the contract's financial transactions, privacy is accepted as a human need and total transparency must be avoided.

The extensive literature review on blockchain explains its key features for financial transaction; transparency and immutability. Blockchain smart contracts can interplay with, or replace legal contract, and mitigate agency theory issues which increases trust in the principal-agent relationship. The MHC is an evolutionary change proposition to ensure stability because it leaves the legal contract as it provides a smart contract as a supplemental transactional tool.

To implement the MHC architecture in a legislation cryptocurrencies are required for the blockchain smart contract to work. Because there is regulatory uncertainty around cryptocurrencies whereas they are illegal in several countries, regulatory strategies such as sandboxes and safe harbors giving regulatory slack and closer collaboration with innovators to ensure financial stability while searching for the optimal regulation is an elaboration on the design of the MHC.

Key agency theory issues are be mitigated significantly when blockchain smart contract's transparent, open, and immutable properties are leveraged in financial transactions. Information sharing increases when using blockchain because a receipt for a financial transactions is indistinguishable from the transaction itself, thus the MHC provides a deterrent against financial crime by removing the opportunity of conducting receipt fraud. Moreover, the MHC mitigates

moral hazard because auditing the immutable and transparent blockchain-based transactions does not require trust in the auditor because the process can be automated by automatically reading data from the blockchain smart contract. Thus agency costs are also reduced as the monitoring costs of financial transactions are reduced, and blockchain smart contracts replace auditors.

Acknowledgments

First, I want to thank my supervisors Roger Sørheim and Donn Morrison for providing guidance. I also want to thank Emil Sina Emami, Andri Karoline Lunøe Spilker, Svein Grimholt and Stian Sandø for proof-reading this paper and providing valuable feedback. Thanks to blockchain experts Jakob Svennevik Notland, Ken Siva Lie, Alf Johansen and Håvard Kittilsen for being insightful and delightful discussion partners on the topic as we simultaneously finished our theses on the same topic; blockchain, spring 2019.

1 Introduction

While the fall of the Soviet Union marked the end of the discussions regarding the type of financial institutions a country ought to implement, discussion for the last three decades have revolved around discovering, and implementing the ideal mechanisms for achieving the established ideal, which is a free market economy. At the heart of these debates has been the question of how a free market economy can be both secure, accountable, transparent and inclusive to the actors involved, with the solution to these issues being contract and financial regulations. Inclusive.

However, the precarious nature of contracts and existing financial regulations were brought to the surface when several Brazilian politicians got arrested for "Operation Car Wash" in 2015. The scandal, which is still under investigation at the time of writing, is estimated thus far to have resulted in a total loss of $13.8 billion in lost tax revenues (Global Witness 2018; Figueiredo 2016). Importantly, scandals like this are not limited to emerging economies of non-western states, as was made evident when it was revealed that Danske Bank was involved in facilitating the biggest money laundering scheme in human history involving $230 billion (Milne & Winter 2018). As a result, the world today is experiencing what has been defined by Edelman (2017) as a trust "trust crisis," which reached its nadir in 2017, but remains relatively low in most of the world today (Edelman 2019).

While understood to be necessary for political, social and financial stability, the plethora of laws, directives and regulations emerging from state bureaucracies and international organisations have in many respects failed to prevent corruption and financial crime, while also contributing to stifling innovation and cause regulatory insecurity to startups and new emerging actors in the market (Department of Justice 2014; KYC360 2016; Stacher 2018), thereby failing to reach their objectives of optimising the free market economy.

By limiting the scope of smart contracts exclusively to financial transactions, this paper, therefore, proposes an evolutionary─as opposed to revolutionary─change to the legal contract as a practical and realistic solution to existing problems, where a smart contract supplements the legal contract. The product of this synthesis is the Minimum Hybrid Contract (MHC) which seeks to implement the accountability and transparency of smart contracts into the realm of human judgment and discretion, which governs legal verdicts today.

This thesis will demonstrate that using blockchain technology as a supplement can improve legal contracts. In Chapter 3 Under agency theory "moral hazard," "agency costs" and "information asymmetry"─which will be explained in detail below─ is defined as recurrent issues in contractual relationships, which this thesis sets out to overcome using blockchain technology. The argument advanced here is that in addition to using a court for legal disputes in contractual relationships, supplementing the legal contract with blockchain as a tool for setting the rules for financial transactions can yield benefits. Correctly, subsequently, the discussion in chapter five will argue that doing so provides transparency, immutable transactions while also lowering the cost of conducting due diligence and auditability assessments by lowering the cost of information sharing.

The Research Questions (RQ) of this thesis are, therefore:
RQ1: How can traditional legal contracts become more trustworthy?
RQ2: How can blockchain technology improve existing contractual frameworks

In what follows Chapter 2 will provide a general discussion on corruption in contracting as basis as a contextual basis for the theoretical framework of this thesis; agency theory. It will use agency theory to focus on the contractual "principal-agent relationships," and how trust, transparency, and information sharing in the light of agency theory affects its outcome. Chapter 5 argues that MHC is an excellent governance tool for optimal information sharing in agent-principal relationships. By reaching optimal information sharing and to reducing

information asymmetry, it will show how increased transparency and trust as understood in agency theory terms can reduce the agency costs or risk-sharing and monitoring.

Having done so, Chapter 3 provides a literature review of agency theory and the principal-agent relationship, and Chapter 4 will provide a literature review of blockchain technology, with particular reference to cryptocurrency as a form of money controlled by anyone with a device and internet connection. "Bitcoin," the first cryptocurrency will be used to demonstrate how the largest and most battle-tested blockchain works, while the negative sentiment around cryptocurrencies and how its seen as a criminal gambling object in the media will also be addressed. Then the concept of smart contracts will be explained to provide a conceptual explanation for how public-private key cryptography is used as addresses for receiving and for authentication for signing and approving cryptocurrency transactions.

Chapter 5 will provide an overview of how an MHC can be designed to answer RQ2. Here generally how legal contract can be forged in a one-to-one relationship with a legal contract and how they interact is explained. Public-private key pairs are used for authentication and attribution to whom approved transactions and transactions are openly and immutably available for auditors. The legal contract is still used for settling disputes and declaring the legal text and a smart contract, and its capabilities are leverage for conducting transactions. Chapter 5 will look at the MHC as a potential tool for solving agency issues and mitigate trust in agent-principal relationships laying the foundation for answering RQ1. Then there is a meta discussion on how MHCs affects agency theory focusing on the principal-agent relationship and its effects on the relationships based on hand-picked propositions by Eidenhard (1989). Finally, Chapter 5 discusses how regulators can proceed with regulating the MHC as an elaboration on the design of the MHC further answering RQ2 as regulatory compliance is required for the MHC to be legal.

2 Context

The 2017 Edelman trust barometer discovered that trust in institutions, including NGOs and corporations, have in 2016 declined to trust "lows" similar to trust levels during the financial crisis. 85% of respondents indicated that it does not "trust the system." Moreover, only 52% of the respondents trust in businesses (Edelman 2017). Trust is now higher than in 2017 but remains relatively low in most of the world (Edelman 2019).

In what follows, this chapter will present a context section first focusing on corruption literature in contracting as a backdrop for agency theory and the discussion. Although this thesis will focus on corruption in contracting in general, Brazil will be used as an illustrative case for discussion and background. The corruption case in Brazil is well documented, recent, and it overlaps with the corruption literature from contracting as governments issue such contracts frequently (Hayne 2017).

2.1 Corruption

The 2017 Edelman trust barometer discovered that trust in institutions, including NGOs and corporations, have in 2016 declined to trust "lows" similar to trust levels during the financial crisis. 85% of respondents indicated that it does not "trust the system." Moreover, only 52% of the respondents trust in businesses (Edelman 2017). Trust is now higher than in 2017 but remains relatively low in most of the world (Edelman 2019).

In what follows, this chapter will present a context section first focusing on corruption literature in contracting as a backdrop for agency theory and the discussion. Although this thesis will focus on corruption in contracting in general, Brazil will be used as an illustrative case for discussion and background. The corruption case in Brazil is well documented, recent, and it overlaps with the corruption literature from contracting as governments issue such contracts frequently (Hayne 2017).

The most extensive literature in contract fraud regarding corruption focuses on the construction industry. Construction industry contracts in the United States have been documented to experience a fraudulent trend as the fragmented nature of the industry makes it challenging to trace payment information (Ahmad et al. 1995; Kenny 2009). Nevertheless, such corruption mostly arose from a lack of transparency and was estimated to have reached approximately USD 340 billion in 2008. Since the global construction market is valued at around USD 3.2 trillion, this means that approximately 10% of the total market value was corrupted, thereby revealing that corruption is not an anomaly, but instead a significant problem of an essential industry in one of the world's most developed economies.

According to Sohail and Cavill (2008), the primary reasons for corruption in the construction sector in the US has been attributed to:

> (1) overcompetition in the tendering process, (2) insufficient transparency in the selection criteria for tenderers, (3) inappropriate political interference in cost decisions,(4) complexity of institutional roles and functions, and (5) asymmetric information amongst project parties.

Other relevant cases of contract fraud in the construction industry appear to takes form as misinformation by withholding information, misleading, and altering documents. Other malpractices such as making payments and invoices for materials never received is also prevalent. (Heuvel 2005; Bowen et al. 2007). For example, two surveys conducted in South Africa and Australia has shown that deceit and misinformation are the most common types of fraud (Vee & Skitmore 2003).

Moreover, the Danish Institute for International Studies has shown using the World Bank Governance Indicators that the countries situated in the bottom 20 percentile on corruption control are also the most fragile states (Orre & Mathisen 2008). States characterized by the weak central government and political instability also experience high levels of corruption (Foreign

Policy 2008). States with these characteristics are often defined as developing countries, which according to The World Bank and the United Nations Office of Drugs and Crimes (UNODC), are estimated to lose USD 20-40 billion due corrupt practices (UNODC 2010). One of the direst statistics can be seen in the estimates of the African Union, which suggests that USD 150 billion (25% of the continent's GDP) is lost every year due to financial malpractices (Transparency International 2007).

2.2 Illustrative Case: Brazil

As mentioned in Chapter 1, corruption is not limited to the developed world but also a characteristic of emerging economies, as well as countries rich in natural resources. When resource-rich countries have lousy performance in socio-economic development or a "resource curse," corruption is seen as a critical factor in explaining it (Mehlum et al. 2006; Robinson et al. 2006; Ross 2001). An example that both qualifies as an emerging market, and a "resource cursed" country, and I have chosen Brazil as an illustrative case for this thesis in order to demonstrate how and why the relevant cornerstone capabilities of blockchain are relevant for corruption.

While the Danske Bank corruption scandal and the Panama Papers (Obermayer Obermaier 2016) suggests that the extent of corruption in the West is yet to be revealed, Brazil makes a particularly useful case study due to its well documented corruption scandal which emerged in 2014 with unprecedented judicial and political repercussions, called "Operation Car Wash" (Portuguese: Operação Lava Jato). The scandal uncovered large scale money laundering, kickbacks, and bribery, which has been estimated to result in a loss of $13.8 billion in lost tax revenues. Public contracts were overcharged and channeled back to the pockets of politicians, their political campaigns, parties, and other bureaucrats (Global Witness 2018; Figueiredo 2016).

Specifically, Brazilian politician Eduardo Cunha has been indicted for taking bribes of around USD 1.8 million connected to Operation Car Wash. Several public officials also accepted bribes in return for handing out inflated, fraudulent contracts which supplied various goods and services

to Petrobras, a huge state-run oil company. The 35th president of Brazil Luiz Inácio Lula da Silva, known as "Lula," wrote a "Letter to the Brazilian People" where he promised that if he won (which he did), he would secure the country's economic stability and honor contracts (Melo 2016). Following the revelation of Operation Car Wash, Lula is now serving a 12-year prison sentence for passive corruption and money laundering (New York Times 2018).

The financial contracting environment in Brazil, therefore, appears unreliable to financial actors. Indicators of country risk have consistently rated Brazil as moderate to high risk due to its weak institutions, an interventionist state, high inflation, and volatile real-sector activity (Anderson 1999). What is more, Business infrastructure in Brazil is also in a fragile state, as was made evident in PWC's report, which outlined factors for contracting/business deal failure in Brazil (PWC 2017):

- Excessive legal formalities/bureaucracy
- Low quality of available information
- Insufficient due diligence before investment
- Overestimated synergy/restructuring gains
- Inefficient post-acquisition monitoring

In addition to the factors mentioned above, Brazil also suffers from accounting practices dominated by legal and administration systems inherited from Spanish and Portuguese colonizers (Ball 1995). These arguably outdated practices have blighted the quality of disclosure in Brazil, despite financial statements being required by law to be audited, but rarely relied upon (da Costa 1993; Silvia & Colauto 2016). Consequently, it is common practice for firms in Brazil to have financial statements which do not correspond to the reality of their operations, with both the records of small and large firms commonly subjected to manipulation (Silva 1990; Silvia & Colauto 2016). Therefore, while the five largest auditing firms audit fraud in the USA at a rate of 91%, the percentage in Brazil was 32% (Silva & Cardozo 2012). Despite being written in 1993, da Costa's (1993) argument that faulty information combined with a regulatory framework

which is often not enforced by the state means that auditing standards are lower than the developed countries it is aiming to compete with remains true nearly 30 years later.

Seeking to solve these issues, in 2014, Brazil implemented an anti-bribery and corruption act (Lei No. 12.846 2013) known as the "Clean Company Act." This law provides severe administrative and civil responsibilities for companies who commit or are involved in fraud or corruption involving a domestic or foreign public official. The law also includes a successor liability clause were acquiring companies are responsible for the misdeeds of acquired companies (GAN 2019). However, as Ball (1995) argues, in order to regain public trust, Institutions in Brazil also need to reduce the costs of enforcing contracts, defining property rights, and measuring attributes of exchange. The most relevant organizations and Ball recommends for reform are:

- Juridical enforcement such as a law court or judge and quasi-judicial enforcement such as an arbitrator.
- Practices for accounting and disclosure.
- Credit rating agencies, appraisers and auditors
- Regulatory bodies to promote market integrity

Using agency theory as an analytical lens, the remainder of this paper will utilize blockchain to achieve these objectives and present an alternative remedy to the symptom that has blighted not only Brazil's economy but the world economy as a whole.

3 Theoretical Framework: Agency Theory

The relationship investigated in agency theory is one of the most commonly codified and oldest codes of social interaction. Agency theory revolves around the "principal-agent" relationship, where a "principal" hires an "agent" using a legal contract. As the "principal," delegates work to another, the "agent" (Eisenhardt 1985), with the agent thereby acting on behalf of the principal in a particular decision problem domain (Ross 1973).

In what follows, this chapter will first outline the principal-agent relationship and it's problem domains outlined in agency theory, here it will argue that there is a difference in how much risk the principal and agent is willing to take and that their goals might differ. Having done so, it will examine information asymmetries between agent and principal and how the principal want to avoid subsequent agency costs. Finally, it will illustrate how organizations are seen as a nexus of contracts and transparency in contractual relationships.

Agency Theory Overview	
Key idea	Principal-agent relationships should reflect efficient organization of information and risk-bearing costs
Unit of analysis	Contract between principal and agent
Human assumptions	Self-interest Bounded rationality Risk aversion
Organizational assumptions	Partial goal conflict among participants Efficiency as the effectiveness criterion Information asymmetry between principal and agent
Information assumption	Information as a purchasable commodity
Contracting problems	Agency (moral hazard and adverse selection) Risk sharing
Problem domain	Relationships in which the principal and agent have partly differing goals and risk preferences (e.g., compensation, regulation, leaderships, impression management, whistle-blowing, vertical integration, transfer pricing)

Figure 1: An overview of agency theory (Eisenhardt 1989).

3.1 Principal-Agent Relationship

The essence of agency theory is the study of principal-agent relationships such as lawyer-client, buyer-supplier, and employer-employee, to name a few (Harris & Raviv 1978). The principal-agent literature intends to construct a blueprint for an optimal contract between principal and agent. Eisenhardt (1989) shows that the problem domain studied in the principal-agent relationship is where the principal and the agent have different preferences for what the goal of the relationship is, and how much risk they are willing to take. For example, how much the agent should be compensated if one party prefers to whistle-blow when there are illegal practices in the relationship. Therefore, it is assumed that the principal and agent have different goals, and "goal-conflict" is thus assumed.

As the study of agent-principal relationships started to receive more scholarly attention in the 1960s and early 1970, studies on risk sharing in individuals and groups revealed that the risk-sharing problem arises when cooperating actors have different attitudes towards risk (Arrow 1971; Wilson 1968).

Another aspect of the principal-agent relationship is what is known as "Moral hazard," which refers to the lack of effort in the side of the agent, argues that an agent can not make the agreed-upon effort and neglects contractual responsibilities. For example, moral hazard occurs if a research scientist uses company time to work on a personal research project. The personal project could be so complex that corporate management fails to detect that what the scientist is actually doing in company time. This violates the interests of the management (principal), and moral hazard occurs (Eisenhardt 1989; Holström 1979).

"Adverse selection" is another aspect concerned with the possibility for a principal making a misinformed decision regarding the choice of agent. An Agent can claim to have certain skills and abilities when signing a contract, but adverse selection occurs since there is no way to completely verify the skills and abilities of an agent on the job or when hiring an agent. If a

research scientist that claims to have experience in a field and an employer is incapable of judging whether this is the case, adverse selection occurs (Eisenhardt 1989).

In many respects, agency theory functions as an attempt to solve issues related to trust mostly discussed as an absent factor, which it seeks to replace with an optimal contractual framework. In doing so, it intends to allow clear communication and acceptance of taking risks and experimenting (Golembiewski 1979; Carnevale 1995). What is more, trust is also valuable in agency theory as it is in the principal's interest to develop trusting relationships with agents as this reduces the need to spend resources on monitoring the agent, thereby making the relationship more cost effective for the principal (Shankman 1999).

3.2 Information Asymmetry

It is rational for a principal and an agent to enter into an agency relationship when there are information asymmetries. Information asymmetry occurs when either; (a) An agent has competencies or general information to complete a task that the principal does not possess, or;(b) both have the same competencies, but the agent has the opportunity to complete the task at a lower cost. (Pratt & Zeckhauser 1985). The claim is that agency theory can contribute to an overall framework for placing various forms of self-interest in corporate behaviors such as lying and secrecy (Sitkin 1987) and blame (Leatherwood & Conlon 1987). This can lead to a better knowledge when the behaviors above are effective, and moral hazard and adverse selection occurs (Eisenhardt 1989).

Identifying the optimal choice between these two options is determined by finding the optimal trade-off between the cost of monitoring behavior and the cost of outcome measurement, and shifting risk to the agent. The agent is assumed to have a stronger dislike and opposition to risk than the principal and is seen as "risk-averse." Agency theory also assumes that the result or outcome of the agent's action is easily measured while the agent's actions leading to the outcome is hard to measure (Eisenhardt 1985).

When a principal cannot monitor competencies before and after the fact, and map out the agents' intentions beforehand, there is information asymmetry. It also arises when knowledge of an agent's behavior is unclear and not deemed trustworthy. As mentioned above Eisenhardt (1989) notes that agency theory regards information as a commodity: Information has a cost and can be purchased and organizations can invest in information systems to control opportunistic behavior from the agent. The commodity principle requires information to monitor the agents' effort in behavior-based contracts, and pay him accordingly in outcome-based contracts. Information on environmental processes or states can also influence an agents' performance and is thus needed by the principal.

Arrow's (1962) information asymmetry paradox where information is regarded as a commodity which can be bought and sold sheds light on the key problem in information transfer:

> The information buyer does not know exactly what he is buying, but if the seller were to provide the potential buyer with that information, he would be transferring it free of charge. In such circumstances, the ownership advantage the supplier has in an asset would be given away without any gain.

Another aspect of information asymmetry can be seen in the transfer of tacit knowledge which knowledge that is hard to transfer to other people by verbalizing or writing it down. Understood as the knowledge that is difficult to transfer by verbalizing or writing it down, and cannot be stated on a technical drawing, such as financial records or a patent. Tacit knowledge needs to be transferred from person to person, and it is intangible, and hard to put a price on using market mechanisms, Hennart (1989) notes that:

The higher the tacit component in the technology package and the weaker the legal protection afforded to innovators, the less efficient markets will be in effect the transfer.

Many cases are used to describe the information asymmetry approach (Demski & Feltham 1978), such as these two outlined by Eisenhardt (1989):

1. Complete information

   The principal knows what the agent has done. Given that the principal is buying the agent's behavior, then a contract that is based on behavior is deemed efficient. An outcome-based contract would needlessly transfer risk to the agent, who is assumed to be more risk-averse than the principal.

2. Incomplete information

   The second case is when the principal does not know precisely what the agent has done. Given the self-interest of the agent, the agent may or may not have behaved as agreed. The agency problem arises because (a) the principal and the agent have different goals, and (b) The principal cannot determine if the agent has behaved appropriately.

When a principal has incomplete information about an agents behavior, it has two options to control it. Eisenhardt (1985) notes:

1. Monitoring behavior:

   The principal can purchase information about the agent's behavior and reward those behaviors. This requires the purchase of surveillance mechanisms such as cost accounting measures, budgeting systems, or additional layers of management.

2. Rewarding outcome:

   Alternatively, the principal can reward the agent based on outcomes (e.g., profitability). Such outcomes are surrogate measures for behaviors. However, in this option, the agent it penalized or rewarded for outcomes partially outside his/her control. In other words, good outcomes can occur despite small efforts, and poor outcomes can occur despite reasonable efforts. While this scheme encourages effort on the part of the agent, it does so at the price of shifting some of the risks of the firm to the agent

Figure 2 provides an overview of the principal-agent relationship when information asymmetry is added. The principal (P) hires the agent (A) which subsequently performs actions. Asymmetric information and self-interests of both parties give way for "moral hazard" and "adverse selection."

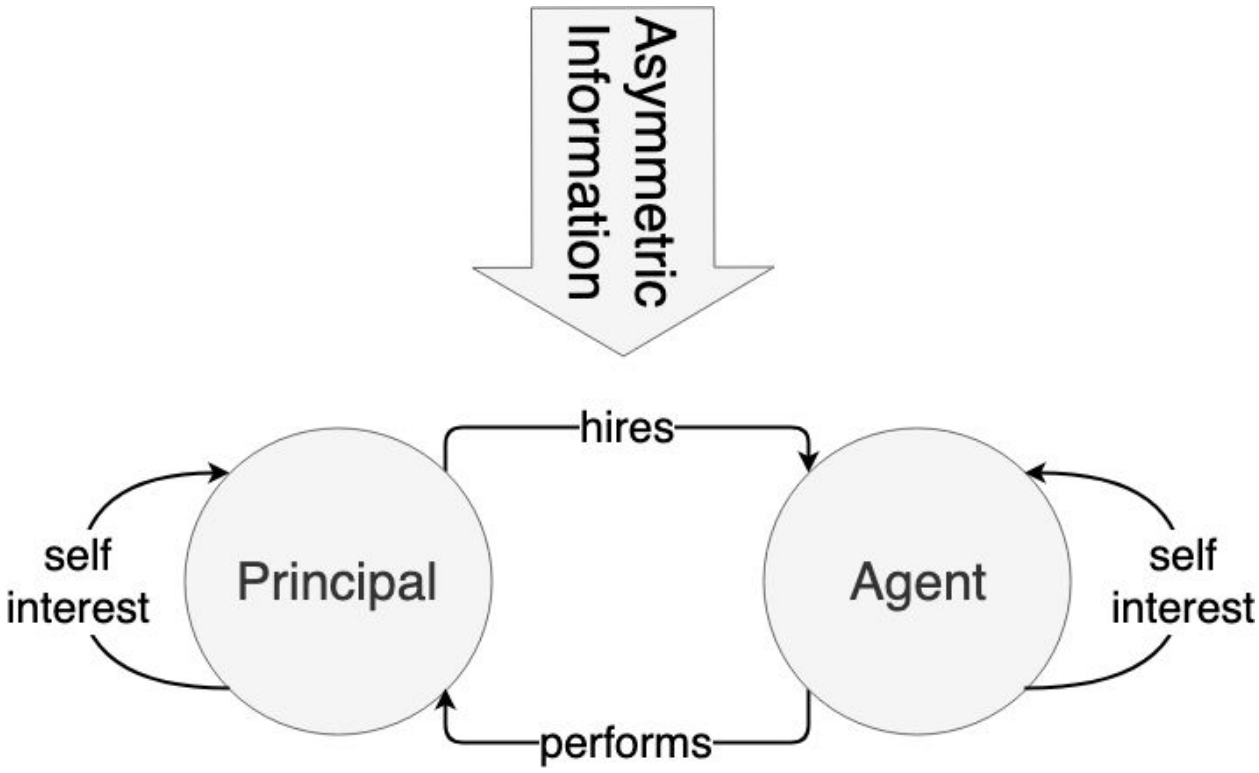

Figure 2: Principal-agent relationship flowchart.

Scholars have highlighted the basic need of information sharing if supply chains are to increase their performance on a supply chain which contains several contractual agent-principal relationships (Stank et al. 1999; Lambert & Cooper; Lau & Lee 2000). This has been coined by Mason-Jones and Towill (1997) as "information enrichment," or the instantaneous sharing of data from the marketplace with all actors in the supply chain is not only desirable but mandatory. "Information enrichment" needs to be achieved in a process integration scenario where the goal is reaching a "seamless" supply chain where all "players" act and think as one (Towill 1997).

However, "information enrichment" raises the issue of privacy and the issue of ownership of information. Concerns about information privacy constitute an obstacle to interpersonal sharing of information in supply chains, the question of what information can be shared with third parties. To foster interpersonal information exchange in supply chains, scholars such as Razavi

and Iverson (2006) have argued that a trusted network where individuals can share information should be built. While this issue has been highlighted in agency theory, no optimal solutions have been provided as of today. Chapter 5.2 argues that this can be solved through blockchain using the MHC. This argument was created before the concept of Bitcoin (and eventually blockchain) was conceived in 2008 (Nakamoto 2008).

3.3 Agency Costs

> The directors of such [joint-stock] companies, however, being the managers rather of other people's money than of their own, it cannot well be expected, that they should watch over it with the same anxious vigilance with which the partners in a private copartnery frequently watch over their own. Like the stewards of a rich man, they are apt to consider attention to small matters as not for their master's honur, and very easily give themselves a dispensation from having it. Negligence and profusion, therefore, must always prevail, more or Iess, in the management of the affairs of such a company (Smith 1776).

"Agency costs" in agency theory expands Adam Smith's (1776) "theory of the firm" by addressing the problem of a black box of the firm, whereas merely changing the inputs changes the outputs. The theory stems from investigating the behavioral implications of property rights specified in legal contracts between owners (principals) and managers of firms (agents). Agency costs occur in principal-agent relationships when the agent has an incentive to perform differently than in the best interest of the principal. The principal cannot observe the actions of the agent and imperfect information sharing leads to a moral hazard problem, and thus marked the probability for an agent acting in a principal's interest lower. Jensen and Meckling (1976) argue that agency cost occurs in a principal-agent relationship when:

> ... there will be some divergence between the agent's decisions and those decisions which would maximize the welfare of the principal. The dollar equivalent of the reduction in welfare experienced by the principal due to this divergence is also a cost of the agency relationship, and we refer to this latter cost as the "residual loss". We define agency costs as the sum of:
>
> 1. The monitoring expenditures by the principal
> 2. The bonding expenditures by the agent,

3. The residual loss.

Agency Costs includes stakeholders in corporate governance such as management, owners, and other stakeholders such as government acting as principals and agents in various relationships. Organizations are mostly seen as "legal fictions which serve as a nexus for a set of contracting relationships among individuals." For example, if corporate management (agents) seeks to spend money on wasteful pet projects and acquiring companies to expand power instead of maximizing shareholders (principal) agency costs occur. This can also affect the population of a political district (the principal) if a politician (the agent) passes legislation which is helpful to large donors and their political campaign, but not the voters (Jensen and Meckling 1976). Better information sharing has been a widely suggested solution for reducing agency costs (Claus & Kim 2004), something which Chapter 7 will demonstrate being possible using blockchain technology.

3.4 Organizations and Governance

Organizations are often understood to be the nexus of contracts in agency theory and are perceived to have two key features. The first one is the divergence of preferences among organizational members, as people's preferences for their actions are not necessarily aligned with the preferences of the organization members. This view of an organization puts the role of rewards and control measures in the hands of actors, assuming that their self-interest will align with the interest of the collective. If there is no divergence between outcome and behavior, measurement is unnecessary for control (Eisenhardt 1985).

The second key feature is the outcome uncertainty of organizations, whereas organizations futures are assumed to be uncertain. The future of an organization can bring both bankruptcy, prosperity, and a myriad of intermediate outcomes. Principals (owners) in an organization bear part of the risk, but agents (employees) carry increasing risk as principals control measures become outcome-based. In this view, rewards and control system measures both motivate

behavior and alter risk sharing patterns at the same time. However, organizations are not only viewed as risk sharing systems but also work sharing collectives (Eisenhardt 1985).

Organizational approaches to control (e.g., Ouchi 1979) suggest two underlying control strategies. On the one hand, control can be accomplished through performance evaluation. Performance evaluation refers to the cybernetic process of monitoring and rewarding performance. This strategy emphasizes the information aspects of control. Namely, to what degree can the various elements of performance be assessed? Alternatively, control can be achieved by minimizing the divergence of preferences among organizational members. That is, members cooperate in the achievement of organizational goals because the members understand and have internalized these goals. This strategy emphasizes people policies such as selection, training, and socialization. The two control strategies are interrelated. An organization can tolerate a workforce with highly diverse goals if a precise evaluation system exists. In contrast, a lack of precision in performance evaluation can be tolerated when goal incompatibility is minor (Ouchi 1979). The ease of performance evaluation drives the choice between the two.

What governance is optimal for one firm at a certain point in time is not necessarily optimal for another. In respect to agency conflicts and despite its faults, McColgan (2001) argues that the modern corporation is the most popular form of organization. This could be mostly attributed to governance mechanisms seeking to limit agency problems. Devices such as the modern corporation should continue to evolve, and further research should focus on understanding what, when, and why they work.

According to Denis (2001), a country's legal system sets the premise for how its governance system evolves. He argues that two conditions ensure effective governance mechanisms; (a) Governance serves as a device to narrow gaps between shareholders' and managers' interests, and; (b) meaningful relationships between mechanisms, performance and value can be observed, if firms are in equilibrium with their governance mechanisms.

3.5 Transparency

There is currently no consensus on the definition of transparency in agency theory (Kaufmann & Bellver 2005; Arajo & Tejedo-Romero 2016). Narrowing down the definition of transparency used in this paper, the amount, accuracy, scope, and timeliness of information as outlined in Vishwanath and Kaufmann (1999) will be used. Focusing on transparency in economics, the scholar Islam (2003) has developed a transparency index which is based on timeliness and availability of economic data. Verily, this paper uses Kaufmann's (2002) definition of transparency understood as "increased flow of timely and reliable economic, social and political information, which is accessible to all relevant stakeholders" by being relevant, accessible, reliable and of good quality.

Lack of transparency can exacerbate corruption-related problems in economics that are rich in natural resources (Kolstad and Wiig 2009). Empirical evidence which suggests that transparency is associated with less corruption, and greater press freedom has been shown to have strong associations with less corruption (Suphachalasai 2005; Brunetti & Weder 2003). Kolstad and Wiig (2009) note that:

> Several studies argue, however, that the effect of transparency on corruption is not unconditional. In other words, transparency is a necessary, but not sufficient condition to reduce corruption. In addition to access to information, you need an ability to process the information, and the ability and incentives to act on the processed information

A well-known example is from Uganda from the 1990s, where surveys showed that only 13% of education grants reached schools, and the rest was captured in the process by the local government. When the Ugandan government started publishing every monthly grant in district newspapers, there was a substantial effect on grants received by schools. Surveyed in 2001, over 80% of the grants reached a school, on average. Thus the impact of access to information about the grants was positive and statistically significant (Reinikka and Svensoon 2005).

Therefore, in normative terms, access to information and transparency is considered a human right in democratic societies, as it is assumed to constitute a fundamental right to be informed about government actions and the reasons for them. In practical terms, transparency is essential for human development as it provides incentives for inclusiveness and redistribution (Stiglitz 1999)

To minimize moral hazard principals incur in monitoring expenditures, for example, the cost of using external auditors for scrutinizing financial statements. On the other hand, agents can incur bonding cost where they purchase an internal audit to signal to the principal that they are acting in consistency with the legal contract (Adams 1994). Wallace (1980) argues that a principal's costs for monitoring an agent's actions will be reflected in the agent's salary and therefore, agents have the interest to demand monitoring such as internal auditing to reduce the risk of the principal making adverse adjustments to executive compensation.

4 Blockchain Literature Review

An open source and open access blockchain (hereby "blockchain") is practically a distributed database using a standard protocol such as Bitcoin. It is a dynamically updated ledger of records that is accessible for anyone that has an Internet connection. The records are organized into in (Bitcoins case) chunks of 2000-3000 transactions each or a "block." Each block is linked to the previous block using a cryptographic method called a "Merkle three," creating a chain of blocks with all transactions that have ever occurred (Nakamoto 2008). Blockchain enables transparency as the history of all transactions can be open and accessible for anyone. On the other hand, the transactions can be encrypted (Ben-Sasson et al. 2014), enabling privacy and anonymized transactions.

Using a blockchain like Bitcoin, two parties can make an exchange without oversight or intermediation from a third party. The peers can rely on the cryptographic proof for trust instead

of a third party, which strongly reduces counterparty risk. This puts the privacy and control of data in the hands of the individual (McFarlane et al. 2017).

Ross William Ulbricht or "Dread Pirate Roberts" funded an online marketplace for trading narcotics and other illicit items because the Bitcoin blockchain enabled an anonymous and uncensorable payment system without governmental interference (Adler 2018). Thus the whole concept of cryptocurrencies is borderline tabu from the onset. Verily Jamie Dimon, the chief executive officer of JP Morgan, stated in 2017 that: Bitcoin is a fraud and will blow up" (Henry & Irrera 2017). The statement crashed the price of Bitcoin, and subsequently, JP Morgan Securities Ltd (Redman 2017) purchased roughly €3M worth of Bitcoin note shares for their clients. Extreme price volatility also frames cryptocurrencies as dangerous gambling objects and several banks including JP Morgan has outright banned customers from buying cryptocurrencies with credit cards (Aslam 2018) while simultaneously opening a The Blockchain Center of Excellence within the bank and released (JP Morgan 2019).

Thus, banks see blockchain as scary and useful at the same time. Being ripe for disruption, the global financial industry both crumbles and invests. Centralized incumbents of global financially-based power such as the USA are also wary of cryptocurrencies and wants to ban them. As United States Congressman Brad Sherman (D) states:

> An awful lot of our international power stems from the fact that the dollar is the standard unit of international finance and transactions [...] it is the announced purpose of the supporters of cryptocurrencies to take that power away from us (Marie 2019).

Distributed networks such as these account for approximately 43% (Africa) to 70% (Russia/Eastern Europe) of all internet traffic (Hendrik & Mochalski 2009). These networks are peer-to-peer connected and operate on any user's computers without a central server, or other central points of failure or control attackers can leverage to shut down the network.

Therefore, one would have to shut down the internet, in general, to stop blockchain completely. Considering the negative sentiment around the words cryptocurrencies and Bitcoin, the word blockchain has been adopted by the industry to put a silver coating on the subject and explain the technology more objectively. Blockchain is essentially a neutral technology and can be used for mundane and useful tasks without challenging global power or empowering illicit narcotics trade. Blockchain has the capability of conducting transparent and immutable financial transactions. This makes blockchain more reliable than current financial systems with comparatively easily hackable centralized servers with completely closed or lost/deleted internal records.

Blockchain also has mechanisms in place so that all parties can reach a consensus on what the canonical truth is. The trust and power in blockchain are distributed among the stakeholders in the system rather than concentrated in an entity or individual such as a government, bank, or financial institution. However, blockchain differs from traditional financial institutions such as banks and payment networks such as VISA as a centralized authority does not regulate it, and as such, whereas the 'trust in the system' in the case of a credit card provider is trust in an individual or a group of individuals, trust in the blockchain system is trust in a static code and the network it runs on which is owned by its user base (Zheng et al. 2017, Crosby 2016).

By using mathematics, code, and decentralized verification of transactions, blockchain can solve the issue of multiparty contention without having to involve any human. What is more, due to its distributed nature, blockchain also eliminates other variables of trust, such as security. The reason for this is that there is no central authority to steal authentication credentials from and corrupt the system, and unilateral government interference, it is not owned by any institution. Instead, the fundamental premise for blockchain is trust in the code, which is open source.

Parties that have different sets of interests will probably relax contention if public blockchain systems replace untrusted systems and processes since public blockchains are self-administered, self-executing and administrator-free. Instead of a system involving an authority that can control

and corrupt the system, blockchain creates a trusted and decentralized way of managing who owns what, or "the current state of the world."

This is the first time a network of globally distributed individuals can reach agreement or consensus on every transaction that took place in a network since it started. Transactions are protected by mathematical principles making them immutable. Bitcoin is designed to be secure and is an example of a distributed computing system that solves the Byzantine general's problem (Nakamoto 2008). The Byzantine general's problem is when an attacker can easily spawn almost an infinite number of fake network nodes, dominate the network and impose an illicit consensus on what transaction has occurred, known as the Sybil attack (Douceur 2002). The anonymous person or group "Satoshi Nakamoto" combined cryptography and game theory to create a "Byzantine Fault Tolerant protocol" using a reward system for actors contributing to the security of the network.

This mechanism is called "Proof-of-Work" (PoW) and requires actors who want to be rewarded by the system or "miners" to solve cryptographic puzzles that require a lot of computing power. This enables a critical security capability, which makes it too expensive for a business or nation state to perform Sybil attacks as a blockchain system grows. The benefits of cheating are less than the costs. Once a transaction has been executed, it cannot be reverted without breaching the whole, which is extremely expensive, hard to orchestrate, and thus, a breach is extremely unlikely to happen. The transactions are permanently protected by mathematical principles making them impossible to edit and immutable (Nakamoto 2008).

PoW miners have to spend money on electricity and computer hardware to solve a random cryptographic puzzle. Another solution for solving the same problems as PoW solved is "Proof-of-stake" (PoS) where not miners but "forgers" (Popov 2016) stake funds in the form of cryptocurrency instead of solving a cryptographic puzzle thus using less computational power and electricity to secure the system (Nxt 2014). The blockchain development team of the

Ethereum blockchain has planned to switch from PoW to PoS in their Ethereum 2.0 (Named "Serenity") version (EthHub 2019).

When utilizing Blockchain, data is freed from data silos such as in banks, Facebook, and Google. Using this technique for managing data makes it high quality, complete, timely, and consistent while at the same time giving the users control of their information (Werbach 2016). Blockchain also has faster transactions than interbank transactions, which can take several days for clearing and settlement. Transacting on blockchain protocols reduces transaction times to minutes and sometimes seconds depending on the blockchain protocol. The transaction fees also decrease when intermediaries and overhead costs are eliminated for asset ownership transactions (Deloitte 2016). To enable this self-sovereignty crucial public-private cryptography is used to put authentication entirely in the hands of the users.

4.1 Money

In what follows, I will first argue that a cryptocurrency is a new form of money in the context of the history of money from barter, gold, and properties of the state-controlled monetary systems today. Finally, I will illustrate how fungibility is a crucial property of any money and if it breaks down the money system itself loses its value because users can never be sure how much one money unit is worth.

4.1.1 Cryptocurrency

In this section, I will make the simple yet profound argument that cryptocurrencies is simply In this section, I will make the simple yet profound argument that cryptocurrencies are simply money. It is a new form of money technology openly accessible for anyone with a smartphone with internet. Thus, when pure cryptocurrency or smart-contract based solutions are in question both the 2.2 billion adults globally with access to financial services and the 2.5 billion adults without access to financial services are all automatically included as potential users (Chaia et al. 2009). All cryptocurrency is presented as legal money systems still has to recognize it as legal

tender: A payment medium which is valid for meeting financial obligations (The Royal Mint 2019).

What backs money is being accepted by many people. A populace can buy into the illusion of the money as a concept. Thus, if a more significant number of people agrees with the notion of cryptocurrency as money, starts accepting and trust them, cryptocurrency money can become as liquid as fiat money (Swan 2015, 70).

> There are no gods in the universe, no nations, no money and no human rights — except in the common imagination of human beings (Harari 2014).

In this thesis, the definition of cryptocurrency follows from the Oxford dictionary (Oxforddictionaries.com 2005) and the author's description of blockchain:

> A cryptocurrency is money in the form of a digital currency. transactions are verified on a decentralized network based on a consensus protocol.

Cryptocurrencies are intriguing because of the intersection of industries and disciplines spanning the field. There are examples of technology, game theory, geopolitics, energy management, and psychology. Nobody is an expert in all, but one can aspire to grasp the basics of each element.

Cryptocurrencies are currently being more and more accepted as payment for services, goods such as paying for coffee at Starbucks, buying food at Whole Foods (Castillo 2019) or paying a mobile carrier subscriptions at AT&T (2019). A cryptocurrency can be used as a medium of exchange by sending cryptocurrencies such as Bitcoin from one address one individual controls the private key to the address another individual controls the private key. Cryptocurrencies can also be used as a store of value. Bitcoin can, for example, be saved, retried and exchange at a later point in time and when the Bitcoin is retrieved it is predictably useful due to the strong antifragility and immutability of the Bitcoin network (Nakamoto 2008).

Cryptocurrencies such as Bitcoin, which is put a simple form of a smart contract with one functionality: Money. Cryptocurrencies have had a complicated and often negative sentiment in media and public forums. Distributed networks such as "BitTorrent" for file, sharing is historically discussed in comparison to Bitcoin. Both are distributed networks but Bitcoin transfers not data, but value. Thus there is a discussion on how being an alternative form of a network such as Bitcoin and BitTorrent outside of including banks and governments is. Distributed protocols operating freely on the internet is historically received with controversy by industrial incumbents and legislators due to its extensive capabilities challenging closed power structures and information/value flows.

When centralized file-sharing companies such as Napster and eventually the distributed BitTorrent file sharing protocol spread during the end of the 1990s, it ended in lawsuits, jail-time and stifled innovation when essentially these were better tools for sharing information. We now have a better tool for sharing not only information but the value in an open, borderless, censorship-resistant, and neutral fashion. We call it blockchain to explain what theory the innovation behind the first cryptocurrency Bitcoin brought us.

If smart-contracts are to supplement legal contracts, they need to have the power to interact with money to conduct financial transactions. Thus I will argue what money is and show that cryptocurrency is a new kind of money readily accessible by smart contracts. Therefore this thesis will make no strategy or recommendation as to how cryptocurrencies will be procured and bought in the first place and assume all actors mentioned has to access to purchase and use it in smart contracts.

Money is a store of value, medium of exchange, a standard of deferred payment, and a unit of account. "Fiat money" adds a particular socio-economic context such as a country or regulation to the definition (Mankiw 2007). In 1977 long before cryptocurrency existed Hayek advocates in his book Decentralization of Money that a competitive private market for money to replace the

government monopoly of fiat money (von Hayek 1977) should exist. He argues against inflationary money (Economica 1931) and posits a model where any financial institution can issue its currency. In his model, there can be several concurrent currencies. These currencies require the institutions to compete to maintain the value of the money through productive activities (Ferrara 2013).

Initially, non-monetary societies have operated along with the principles of debt and gift economy (Graeber 2011). Trading assets without an abstract representation of value or barter was also used, but primarily between potential enemies and strangers (Graeber 2001). Eventually, many cultures around the world developed commodity money. The value of commodity money derives from the value of the object itself. For example, gold and silver are commodities that have been used as mediums of exchange (O'Sullivan & Sheffrin 2003).

After the second world war, the Bretton woods agreement state issued money based on the gold reserve of the country, or gold-backed national currencies (Mankiw 2014) changed. Many countries fixed the exchange rate of their national currencies to the united states dollar. The dollar was still pegged to gold, and therefore, all currencies pegged to the dollar value had a value in terms of gold (Ipsey 1975).

After the second world war the bretton woods agreement state issued money based on the gold reserve of the country, or gold-backed national currencies (Mankiw 2014) changed. Many countries fixed the exchange rate of their national currencies to the united states dollar. The dollar was still pegged to gold and therefore all currencies pegged to the dollar value had a value in terms of gold (Ipsey 1975).

In 1971 the United States president Richard Nixon ended international convertibility from the united states dollar to gold creating a kind of money (Wong 2016) and in 1976 references to gold were officially removed from the statues of the united states dollar creating a new state-issued currency: Government on-demand issued Fiat money. From this point until the time of writing

the global monetary system is run on this kind of money which is not pegged to anything in the physical world directly and has no intrinsic value (Kiyotaki & Wright 1991).

In fiat money, central banks can introduce new money into the economy by means such as lending money or buying financial assets. For example, in the united states, the money supply grew from $6.407 trillion in 2005 to $8.319 trillion in 2009 (Federalreserve.gov 2009). Commercial banks then use this money for fractional reserve banking. This again expands the total supply of money (Abel & Bernanke 2005). Thus, fiat money is controlled by centralized states and organizations and is a centralized form of money as opposed to the distributed nature of cryptocurrencies such as Bitcoin.

4.1.2 Fungibility

As defined by the Oxford dictionary: "Fungible (...) replaceable by another identical item; mutually interchangeable". In the context of money, fungibility means that all unit of a currency such as dollars or Bitcoin is interchangeable for precisely one of any other unit. The bottom line is that if fungibility breaks down, the money itself is unusable and therefore regulators have to process with caution not to break fungibility when regulating cryptocurrencies. If fungibility is destroyed, the basic premise for smart contracts conducting cryptocurrency transaction is lost. Consider the following case as an example of how fungibility almost was destroyed to illustrate why it is deemed as a prerequisite for any form of money fiat or cryptocurrency to maintain its integrity.

In the court case following the incident, the judge ruled in favor of the bank where the note appeared, and the note would not be returned to Crawford. The court argued that if notes that were stolen were to be returned, then it's fungibility and potentially the fungibility of all other notes would be destroyed. This is because if Crawford had received the note, no merchant would ever take the risk of accepting a banknote unless they knew the full transactional history of it. This problem would damage the "currency" of the financial system and the premise for money in general. It would require merchants to pour through newspapers to verify that the note was

legally obtained and the serial number not announced as a "criminal note" (Reid 2013). Thus making it extremely impractical to conduct transactions while simultaneously not being sure what one paper note is actually worth in comparison to the rest.

In the court case following the incident, the judge ruled in favor of the bank where the note appeared and the note would not be returned to Crawford. The court argued that if notes that were stolen were to be returned, then it's fungibility and potentially the fungibility of all other notes would be destroyed. This is because if Crawford had received the note no merchant would ever take the risk of accepting a banknote unless they knew the full transactional history of it. This problem would damage the "currency" of the financial system and the premise for money in general. It would require merchants to pour through newspapers to verify that the note was legally obtained and the serial number not announced as a "criminal note" (Reid 2013). Thus making it extremely impractical to conduct transactions while simultaneously not being sure what one paper note is actually worth in comparison to the rest.

In this sense there are currently emerging cryptocurrencies where transactions are private by default, such as Monero (2019) and ZCash (2019), and Dash (2019) where privacy is optional which can be leveraged by the MHC to find a golden middle way in between transparency and privacy.

4.2 Public-private key cryptography

A public-private key pair is a form of digital identity. Simply put public key an address, and a private key is a password used to prove ownership of it. Private keys have to be kept a secret to retain adequate security, and the corresponding public key can safely be distributed openly (Stallings 1990). Thus blockchain uses the public key for addresses of users and private key for authentication for conducting a transaction.

The public-private key pair enables robust authentication because a sender of information over the internet can combine a message with a private key. This pegs a digital signature to the

message. Anyone who received the message can use the digital signature and the proposed sender's public key to verify that the proposed sender owns the private key that was used to sign the message (Menezes et al. 1996).

Entities such as individuals and organizations can share their public key with identity institutions such as the Swiss city of Zug has done using the Uport digital identity solution. Using public/private keys managed in Uport, Zug issues digital citizenship credentials to citizens effectively making the private key the password controlling each citizens identity (Uport 2017).

Digital identity solutions have long been in development, laying aside centralized authentication providers like Facebook and Google authentication. Using a distributed system where the user is in control has recently been allowed by advances in distributed computing. Public-private key authentication and identification systems like Uport has now been realized (Uport 2017). Solutions like these are dubbed self-sovereign identity solutions because no malicious actor can censor the underlying public/private key pairs actions, impersonate or delete them. As long as the private key is protected, the identity is under complete control of its entity and thus is self-sovereign (Tobin & Reed 2017)

Since a public/private key pair is self-sovereign, blockchain uses them to sign transactions and thus authenticate the owner. The owner of the private key is the owner of the cryptocurrency it controls. "Wallet" is currently used by most of the blockchain sector because it relates to a common word used for storing fiat currencies and other valuables. However, it is a faulty metaphor because it is a tool for managing public-private key pairs. Thus a "Digital Keychain" or "Keychain" is a more descriptive phrase, and I recommend using it. There are four different types of digital keychains: software client, hardware device, material and brain (Bitcoin.org 2019):

- **Software Client**

A digital keychain client is a software program that runs on devices with operating systems such as computers, smartphones, or smart tablets. Anyone can develop and build a keychain client, and keychain clients are often released as open-source projects.

- **Hardware Device**

  When a hardware device is used as digital keychain hardware, the device is a secure special purpose hardware device that stores public-private key pairs. Being stored offline most of the time, these keychain devices are considered very safe and very hard to hack. A keychain like this is only connected to the internet via the USB port of a computer and thus has less attack surface and is not as vulnerable as a software client. Up to the time of writing, there have been no verifiable incidents of cryptocurrencies being stolen from a hardware device.

- **Material**

  A digital brain keychain is when the public-private key pair is stored in one's mind by memorizing a twenty-word long recovery phrase which can be used to recover the public-private key pair. If the recovery phrase is forgotten, the person dies or is permanently incapacitated, the corresponding cryptocurrencies are lost forever

- **Brain**

  A digital brain keychain is when the public-private key pair is stored in one's own mind by memorizing a twenty-word long recovery phrase which can be used to recover the public-private key pair. If the recovery phrase is forgotten, the person dies or is permanently incapacitated, the corresponding cryptocurrencies are lost forever.

4.3 Bitcoin

Bitcoin is the classic example for illustrating cryptocurrency. It inherently uses and spawned the concept of blockchain. Bitcoin is a decentralized peer-to-peer open source protocol and has a set of rules written in computer software code that runs on a network of different computers around the world connected over the internet. Several key innovations and capabilities from cryptography have been combined to enable the capabilities of Bitcoin, Including:

Bitcoin is the classical example for illustrating cryptocurrency. It inherently uses and spawned the concept of blockchain. Bitcoin is a decentralized peer-to-peer open source protocol, and has a set of rules written in computer software code that runs on a network of different computers around the world connected over the internet. Several key innovations and capabilities from cryptography have been combined to enable the capabilities of Bitcoin, Including:

- A public and immutable transaction ledger
- Mining using PoW: A distributed transaction verification system
- Distributed issuance of new Bitcoins
- Public-private key cryptography (last section) for authentication and addresses

The Bitcoin protocol is used as a peer-to-peer electronic cash payment system based on cryptographic proof instead of trust using a PoW protocol. Being the first successful cryptocurrency Bitcoin is deflationary, borderless, neutral and not owned or controlled by any state or company (Nakamoto 2008).

To participate in the Bitcoin public ledger, users send and receive Bitcoins by having their keychain clients; public-private key keychains generated by cryptographic hash functions. Transactions in Bitcoin use cryptographic hashing, digital signing, and verification by the miners of the network. The Bitcoin network is an open network, meaning that there is no information to steal and anyone can join to mine or transact in the system by following the rules of the Bitcoin protocol. Apart from the security of the network, there is a concern for the safety of each individual's keychains. This is up to each user to choose to balance between convenience and risk (Nakamoto 2008).

To participate in the Bitcoin public ledger, users send and receive Bitcoins by having their own keychain clients; public-private key keychains generated by cryptographic hash functions. Transactions in Bitcoin use cryptographic hashing, digital signing, and verification by the miners of the network. The Bitcoin network is an open network, meaning that there is no information to steal and anyone can join to mine or transact in the network by following the rules of the Bitcoin protocol. Apart from the security of the network, there is a concern for the security of each

individual's keychains. This is up to each user to choose to balance between convenience and risk (Nakamoto 2008).

4.4 Forking

On a blockchain such as Bitcoin, the code for the consensus layer is the most difficult to change. This is because the consensus layer defines whether each transaction that is appended to a blockchain record by a miner is valid. These rules include checking if data is formatted correctly, how much the miners are rewarded, and managing transactions. Any changes to these rules is a change in the consensus layer and can create a chain split. For examples changes such as deleting unused files and moving things around to increase the readability of the code, also known as refactoring, have no impact on the consensus layer as it does not change the rules of the protocol and is usually adopted instantaneously (Lombrozo 2017).

On a blockchain such as Bitcoin, the code for the consensus layer is the most difficult to change. This is because the consensus layer defines whether each transaction that is appended to a blockchain record by a miner is valid. These rules include checking if data is properly formatted, how much the miners are rewarded and managing transactions. Any changes to these rules is a change in the consensus layer and can create a chain split. For examples changes such as deleting unused files and moving things around to increase the readability of the code, also known as refactoring, have no impact on the consensus layer as it does not change the rules of the protocol and is usually adopted instantaneously (Lombrozo 2017).

For example, if 60% of the Bitcoin miners upgrade their software and 40% do not upgrade their software, there will effectively have been created two unique blockchains forked out of the original blockchain with 60% of the miners. This is referred to as a "chain split" because where 60% of the miners dedicate their computing power to one blockchain network, and 40% of the miners dedicate their computing power to the other blockchain network (Lin & Liao 2017). The Ethereum blockchain has for example hard forked into two blockchains: Ethereum classic (ETC) and Ethereum (ETH) due to the controversy caused by a security breach. A chain split is also

referred to as a consensus fork because the actors in the blockchain fail to reach consensus on what code to use and end up on different versions of it (Lombrozo 2017).

A chain split will also lead to a "coin split" because of the coin distribution, or what public-private key pairs control what addresses will initially be identical in both the blockchains in the old and the new software. From a user who controls the private keys of addresses in for example ethereum, a chain split will lead to control over an identical amount of ethereum in the new ethereum network that resulted from the new rules (Wirdum 2017). This happened when Ethereum was forked into Ethereum classic. Every ETH cryptocurrency on the Ethereum network was copied with equal public-private key ownership into the Ethereum classic ETC cryptocurrency (Ethereum Classic 2017).

4.5 Smart Contract

A smart contract is a piece of computer code that executes on a blockchain and can transfer value. The purest form of a smart contract is a cryptocurrency for transferring funds to other users based on a public-private key pair of digital signatures (Geiregat 2018). On a smart contract, the terms of the agreement are defined by computer code as a set of instructions (Blockchaintechnologies.com 2016), like unlocking value based on certain conditions. When a value is reached, or certain conditions are met, such as when a user with self-sovereign identity connected to the smart contract sends a command, a smart contract executes predefined code which triggers an event such as a financial transaction. It is characterized by being autonomous, self-sufficient, and decentralized (Swan 2015).

Nick Szabo materialized the concept of a smart contract in (1996) before the crucial cryptographic concept of a blockchain needed to make smart contracts work as intended existed. Szabo defines smart contracts as a combination of protocols with user interfaces that formalizes and secures relationships over computer networks. Smart contract applications discussed include contracting, credit and payment systems enabled by cryptography and other security

mechanisms. Relationships can be algorithmically secured from third-party eavesdropping or malicious interference, and breach by principals (Szabo 1997).

Szabo's idea of a smart contract was too hard and fragile to be implemented as an alternative to traditional financial services due to the lack of blockchain at the time and was never materialized. Possibly because the smart contract conceptualized could be breached by principals controlling the centralized point of failure which existed before blockchain was used to make smart contracts — using the current smart contract technology assets and anything of value that can use blockchain as a public or private ledger of ownership. For example, money, pictures, personal data, academic certificates, medical records, supply-chain assets, physical assets like properties, and gold can be bound to self-sovereign identities. Don Tapscott calls this growing network the Internet of Value (Tapscott & Tapscott 2016).

Using this blockchain, smart contracts have evolved. For example, blockchain networks optimized for smart contracts such as Ethereum (Buterin 2013) is being used as a ledger of ownership of assets such as gold. It also facilitates crowdfunding firms and issuing stocks reliably and transparently, providing immutable receipts for all transactions (Ante & Fiedler 2019).

Werbach and Cornell pose in their (2017) duke law journal entry that there are reasons to be skeptical about whether smart contracts can deliver gains over conventional contracts for contract efficiency and flexibility. Even though smart contracts could fulfill its promises, the bigger question is whether smart contracts can do what courts do, only better. They argue that contract litigation plays a fundamental role in our social system that smart contracts cannot replicate.

A contract often is a manifestation of an ongoing relationship and is often more than a one-shot interaction between parties followed by a judicial resolution of a dispute (Macneil 1978). Several scholars argue that business practices around contracts assume that a contract does not clearly

contemplate all the possible scenarios which can materialize (Hart 1988). Before the event, before a particular dispute, and after a contract is signed parties in contractual relationships must expect a renegotiation of the contract, and after the fact, courts must exercise their authority to settle disputes to fill any gaps in the agreed-upon contract (Holmes 1881).

Smart contracts are software programs where the time dimension of interaction between parties is formally stripped away. The uncertain futures of judicial resolution is ignored, yet smart contracts bind real people with real relationships and how their performance unfolds over time, and there is still a possibility of moral hazard and adverse selection. Thus relying on smart contracts is a bet on before the fact formalization, which will never be able to match the flexibility of human decision making (Werbach & Cornell 2017).

Because once written and deployed a smart contract is immutable and enforces itself, it removes the role of courts and authorities as enforcement agents. This means that once the smart contract is deployed, the machinery for its execution is unavoidably set in motion. Such immutability hinders the parties in the contract from affecting the transaction in disputes after the fact unless the smart contract has such a governing mechanism programmed into its code before it is deployed. Ultimately smart contracts cannot supplant the role that law and courts pay. Smart contracts are not a replacement for judicial contract adjudication (Werbach 2018).

To make a smart contract consistent with legal enforcement, the two can be connected. The approach here is to pair smart contracts and contracts explicitly. This idea was explored in the "Ricardian Contract" by the information security expert Ian Grigg in 2004 before the advent of cryptocurrencies while developing the Ricardo digital transaction platform for financial instruments. The Ricardo platform defines its contractual integration solution as having three components:

1. Legal code: The human-readable text in a contract.
2. Computer code: What steps a smart contract can execute.
3. Parameters: Variables for influencing for the computer code execution.

(Grigg 2004).

Grigg's solution never took off and integrating smart and legal contracts in this manner was mostly a theoretical construct. It was not until blockchain was invented and particularly before the ethereum blockchain successfully implemented smart contracts that this approach was rediscovered and gained momentum. There are currently several groups integrating smart contracts and legal contracts. These include a sub-group within the R3 blockchain consortium led by the British bank Barclays (Reutzel 2016, Rizzo 2016), Mattereum (2019), OpenLaw (2017), JP Morgan (2019) and the Hyperledger open-source initiative (Eris:Legal 2014).

5 Discussion

Having identified contracts as the nexus of corruption, and agency theory as the appropriate framework for identifying the weak spots in existing contractual frameworks, this section will demonstrate how the MHC can help reduce corruption utilizing the transparent, open and immutable properties.

In what follows, I answer **RQ2** by outlining the design of a Minimum Hybrid Contract (MHC) which is a practical model for using a smart contract as a supplement to a legal contract for conducting financial transactions. Then I will discuss how blockchain affects agency theory in the case of using a smart contract as a transactional supplement to a legal contract. Here I will argue that key agency theory issues can be mitigated if blockchain's transparent, open, and immutable properties are leveraged in financial transactions. Finally, to address regulation as a part of the design of the MHC further answering **RQ2**, I will discuss regulatory strategies concerning financial innovations and the new regulation of the internet, and give practical recommendations for how regulators and blockchain innovators can proceed in symbiosis.

5.1 Minimum Hybrid Contract (MHC) Architecture

Being a supplement, not a replacement, for existing contractual frameworks, the smart contract will, on the one hand, facilitate safe and transparent transactions, whose records are immutable, while the traditional contract─and the institutions that ensure its validity─ will continue to take care of the required legal framework and disputes. The outcome of this synthesis of conventional legal structures and blockchain technology is the Minimum Hybrid Contract (MHC) which seeks to reduce corruption and enhance social well being by increasing transparency, information sharing, auditability and cut the cost of financial activity.

Current legal contracts are defined in the Oxford dictionary characterized by being:

> A written or spoken agreement, especially one concerning employment, sales, or tenancy, that is intended to be enforceable by law (Oxforddictionaries.com 2019).

While being a feature of ancient history dating back to the ancient philosopher Plato from the ancient Greece empire (Plato 348 BC), eventually modern law and contracting have evolved but it has nevertheless failed to cope with the economic malpractices discussed in Chapter 2.1 (corruption chapter). What is more, existing contractual frameworks leave substantial room for improvement because of the money and financial system used to conduct financial transactions breeds corruption, and has inferior immutability, transparency, control, and information sharing compared to smart contracts. This is why I propose the MHC as an alternative solution to the shortcomings of the existing status quo.

While I coin the concept of MHC in this thesis, discussions regarding synthesizing traditional and smart contracts have been going on for a few years. For example, legal scholar Werbach (2018) has argued that smart contracts can be used to reinforce traditional law by offering new ways to achieve legal objectives. Smart contracts can address issues that obstruct the enforcement of law and increase trust in legal systems. They are capable of serving in legal

compliance with contracts but still faces adoption challenges as it challenges the power of state currently controlling fiat money supply in currencies such as the United States Dollar and is unregulated by default, but also groups and individuals who either legally or illegally are benefiting from the existing status quo. Improving a contract using a smart contract does not mean that it improves the situation and increases trust enough to gain traction; Law, legal institution, and businesses need to work together (Werbach 2018).

The MHC is a continuation of Werbachs (2018) work on blockchain, smart contract, and building an architecture of trust. The architecture of the MHC a practical model based on the supplement type of possible legal and smart contract interactions outlined in the list proposed by Werbach (2018):

1. Supplement: Law is the primary means of enforcement, and the primary value proposition of the smart contract is the gain of an immutable and transparent record. In supplement scenarios, smart contracts do not necessarily replace contracts.
2. Complement: When a smart contract acts as a complement to a legal regime. Any legal system can fail, and sometimes the volume of activity scales beyond the capacity of legal mechanisms to regulate them. A legal system can benefit from better tracking of people and things it regulates. Enforcement lags when incentives are improperly aligned. Thus a blockchain system can step in to fill enforcement gaps through traditional means.
3. Substitute: Substitute: When smart contracts entirely replace the law as the enforcement mechanism.

Based on the aforementioned supplement legal and smart contract interaction outline by Werbach (2018), the MHC connects the legal text and computer code using cryptographic hash functions as whos in Figure 4. The legal contract text and the smart contract computer code is forged into a one-to-one relationship. The legal code includes a cryptographic hash string of the computer code which guarantees that it references the right smart contract. Also, the smart contract includes a cryptographic hash string of the text of the legal contract making the smart contract and legal contract definitively linked, making each contract depend on the other. The

smart contract facilitates the transactions in the MHC; this makes the transactions instantly auditable because each transaction is indistinguishable from a receipt. Thus contractors and auditors can transparently audit the financial performance of the contract, and if there is an after the fact dispute the legal contract is turned to for resolving it (Grigg 2004).

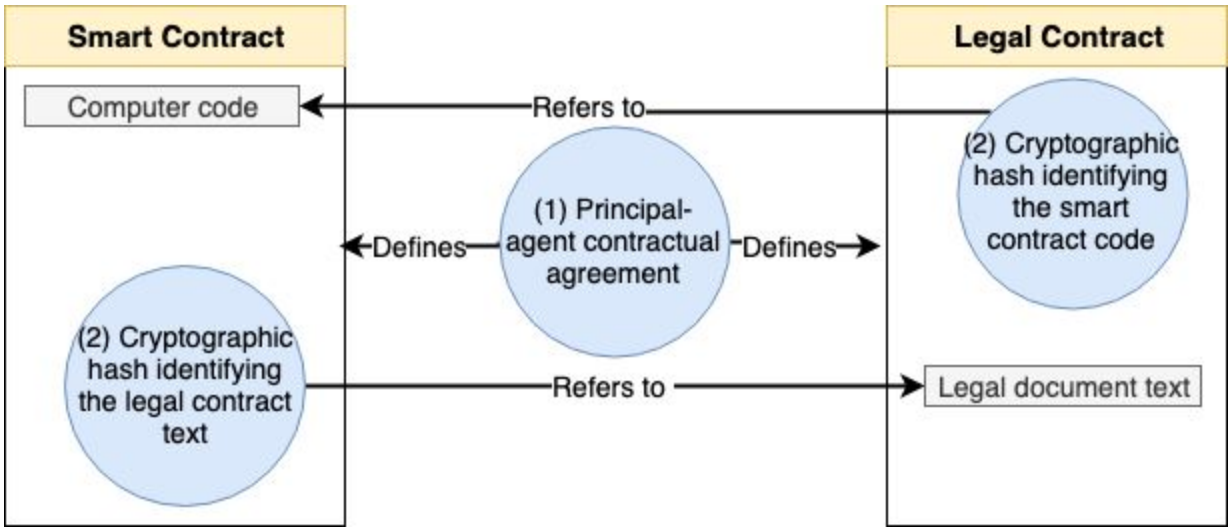

Figure 4: A one-to-one relationships between a legal and smart contract forming the basis of an MHC.

In Figure 4, a principal and an agent signs a contractual agreement. The contracts cross-reference each other. On one hand a cryptographic hash is generated from the legal contract text and written into the computer code of the smart contract. On the other hand a cryptographic hash is generated from the computer code of the smart contract and referenced in the legal document. When a smart contract and legal contract is connected, public-private key pairs are used to authenticate and identify users. A supplemented contract can use computer code in the smart contract to delegate privileges such as transferring funds to certain public-private key pairs.

Each principal and agent hold public-private key pair consisting of their public key (address) and their private key (password), and the public key is used for receiving funds and the private key is used for authorizing transactions. To identify who is the owner of a public key the corresponding identification of the public key (address) of all authorized actors in the smart/legal contract can be stored in a private or government database. Thus, the identity of each public-private key pair

owner is known. Because only the known key pairs can authorize transactions, there is effectively no other way to conduct transactions than using these.

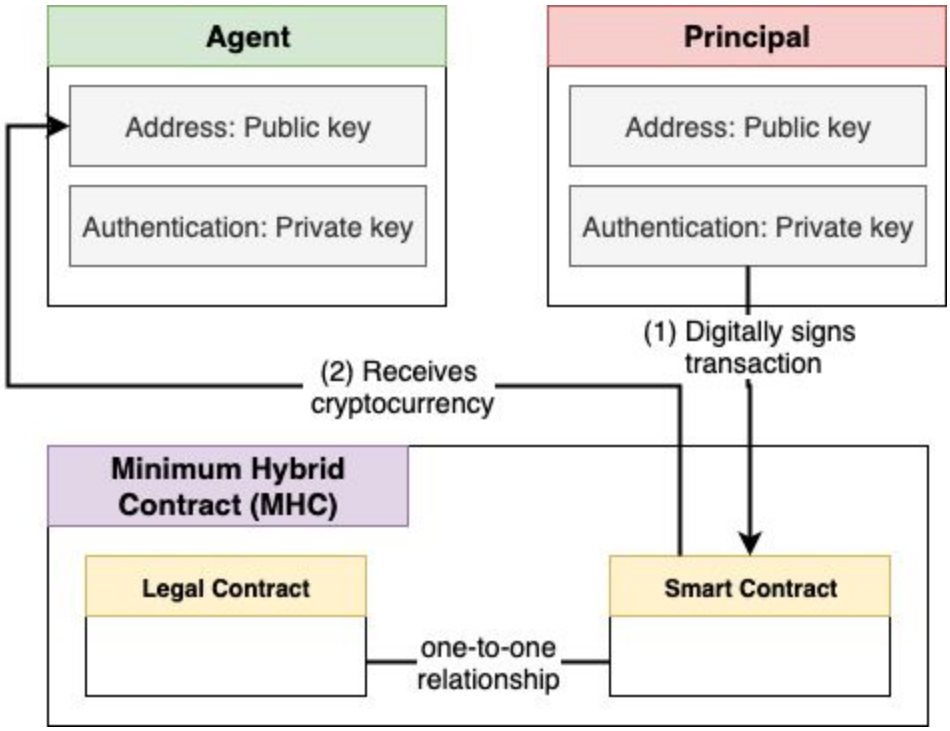

Figure 5: A simple model of a MHC transaction using a smart contract and public-private key pairs.

Figure 5 shows how a transaction is conducted in an MHC. Given the aforementioned one-to-one relationships, the transactions in the smart contract are given legal status. When the principal wants to do a transaction of a certain amount of cryptocurrency, the private key is used for authenticating the transaction. Looking at Figure 5, the transaction is first digitally signed by the principal's private key. Secondly, when the transaction is approved by the blockchain network, the agent address (public key) receives the cryptocurrency. Thus, the cryptocurrency is in the sovereign control of the agent. Only the private key in his possession, which is corresponding to the receiving address (public key), now controls the cryptocurrency.

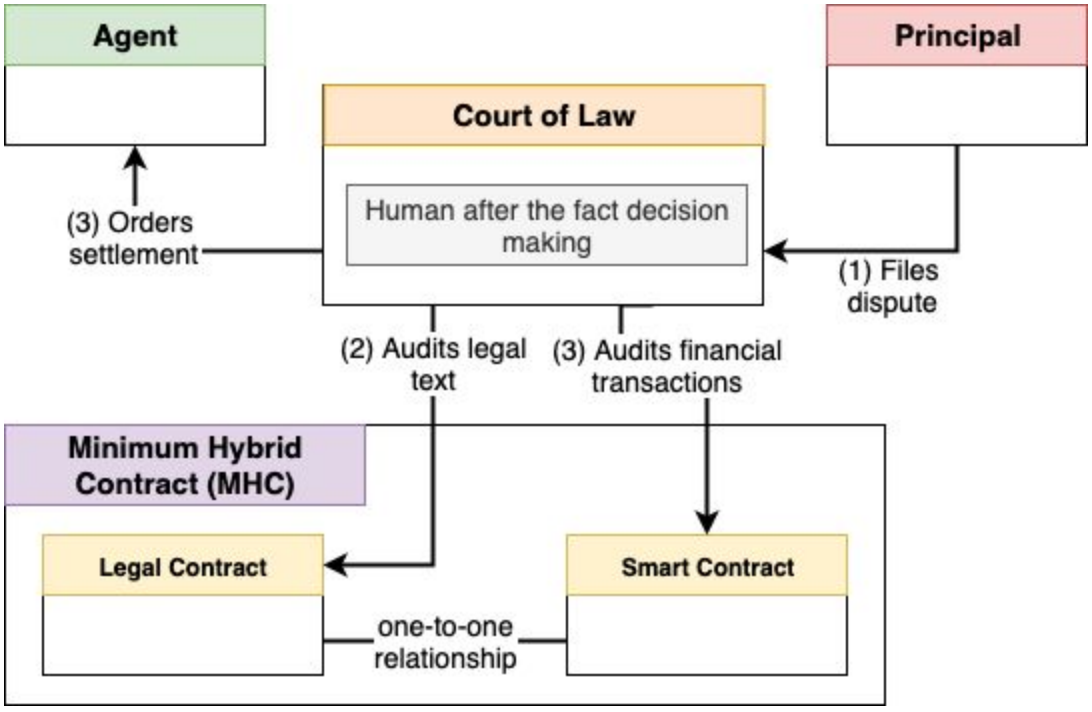

Figure 6: A simple model of the most relevant elements of a dispute in an MHC.

If an organization or individual experiences a contract breach in an MHC after the fact, the transactions in the smart contract cannot be reversed or censored, although it can be used for unveiling illegal and fraudulent transactions. In this case, the dispute is reported to a court which investigates the legal contract and actions taken in the contractual relationship such as transactions which are being openly auditable. If the court orders a financial settlement, the smart contract cannot conduct the transaction of a dispute as a reversal because immutability is a main capability of the smart contract and thus a new transaction has to be undertaken.

If an organization or individual experiences a contract breach in a MHC after the fact, the transactions in the smart contract cannot be reversed or censored, although it can be used for unveiling illicit and fraudulent transactions. In this case the dispute is reported to a court which investigates the legal contract and actions taken in the contractual relationship such as transactions which are being openly auditable. If the court orders a financial settlement the smart contract cannot conduct the transaction of a dispute as a reversal because immutability is a main capability of the smart contract and thus a new transaction has to be conducted.

Smart contracts can directly shape compliance with legal obligations if integrated correctly (Werbach 2018). Therefore, the MHC architecture outlined in this section is chosen as it is the most evolutionary and conservative. This is because I want to make the MHC an iterative suggestion and keep the legal contract intact, thus making the MHC backward compatible with all legal contracts. In addition to that, the MHC leverages the transparent and immutable properties of the smart contract as it conducts the financial transactions. Because of its simplicity, I believe that the MHC is the hybrid architecture regulators most likely will agree with first.

5.2 The MHC and Agency Theory Development

As agency theory primarily revolves around traditional contracts, not all of the concepts and issues discussed in Chapter 5 will be applied to the specialized discussion below. For example, goal conflict in the principal-agent relationship lies outside the scope of financial transactions and will, therefore, not be discussed further. This is because the discussion on goal conflict revolves more around motivation, and I consider changing financial instrument mostly irrelevant for the goals of principals and agents as it does not change their motivation and the nature of the contract. Moreover, MHCs outcome-based contracts will be less affected as agency theory assumes that the outcome of a contract is easily measured. Being able to have less information asymmetry with regards to financial transactions will increase transparency, but as the outcome is assumed to be easily measured this part of contracting is downplayed in this Thesis.

Consequently, Information asymmetries become a critical issue the MHC seeks to solve. As is the case with adverse selection that in several instances, the principal cannot monitor the competencies of the agent. If previous contracts are used for due diligence when a principal is prospecting for potential agents, adverse selection can be mitigated by using financial information from MHC transactions. A principal can demand to audit the transactions ledgers from previous contractual relationships to verify that an agent has conducted the previous contract and not trying to fake last contractual relationships.

Information asymmetries also arise when the knowledge of an agents behavior is unclear. Therefore making financial behavior instantly auditable will help close this financial information gap.

Since information is regarded as a commodity, which has a cost in behavior-based contracts, financial information is usually costly to obtain and flawed as in the cases discussed in Chapter 3. The price of information goes down when using the MHC, as there is no longer need to hire an auditing firm to review financial records and there is no need to trust the auditor and the issuer and safe keeper of the receipt. The principal can make the agent prove which transactions have been conducted using the agent's public-private key pair to prove they were done by the agent and then inspect the transactions using the MHC.

Considering Arrow's (1962) information asymmetry paradox where the buyer of the information cannot know precisely what he is buying, using public-private key pairs in the MHC to prove that a particular individual or organization conducted a transaction shows precisely who did the immutable transaction. On the other hand, in the case of tacit knowledge defined by Hennart (1989), it is not transferred through financial records, and an MHC will not increase the sharing of it.

As in the case of complete and incomplete information, the MHC gives the principal the capability to have full details of all financial transactions conducted by the agent. The principal can use the MHC for budgeting and complete information on cost accounting and complete information in auditing (Eisenhardt 1989). In the case of a principal having incomplete information, Eisenhardt (1985) notes that monitoring behavior is a solution. Here the principal can purchase information and reward them. This is said to among other things require cost accounting systems, as an MHC provides a cost transaction system built into the transactions itself this creates an environment where the information is not necessarily purchased but read of the blockchain transaction ledger directly on the internet.

In agency theory, a supply chain is seen as a nexus of contracts. Using MHCs can increase financial information sharing and improve the performance of the supply chain. MHCs, which can instantly share data, can give the financial part of the supply chain information enrichment. Thus the goal stated by Towill (1997) that all players act and think as one is approached.

The topic of information sharing raises the issue of privacy and ownership of information and what information can be shared with third parties. As for financial information, the MHC is a tool with the capabilities to foster the interpersonal information exchange for supply chains as defined by Razavi and Iverson (2006). They argue that a trusted network where individuals can share information should be built, and now that we have MHCs there are lots of room to experiment and explore. Verily IBM and the shipping giant Maersk is experimenting with a blockchain smart contract project for supply chain "in the name of transparency, information sharing, and innovation" (Takashi 2019).

Considering moral hazard (Eisenhardt 1989; Holström 1979) which is the danger of agent acting contradictory to the principal's interest, the MHC provides a deterrent against financial crime. The MHC offers transparency and immutability for financial transactions, and the receipt for a transaction is indistinguishable from the transaction itself there is zero opportunity to fake receipts, and thus receipt fraud is theoretically impossible. Using the MHC to pool funds for budgeting and using the immutable and transparent transaction in the MHC for cost accounting can reduce the risk of illicit activity because of immutable financial records are available for cost accounting

Considering agency costs where incomplete information leads to moral hazard a principal has to invest in monitoring expenditures (Jensen & Meckling 1976), and better information systems are seen as a cure (Claus & Kim 2004) the MHC has a role to play. As mentioned above the MHC is an excellent financial tool for internal and external auditing, and information about transactions

can be shared instantly and transparently. Therefore, the MHC provides a better financial information system for contracts, which also reduces agency costs.

A principal incurs in monitoring costs such as external auditing, and an agent incurs in bonding costs such as internal auditing to reduce moral hazard (Eisenhardt 1985). These costs can be reduced when auditors are replaced by computers code. Because a principal's costs for monitoring an agent is reflected in the agent's salary using MHC to cut these costs will be reflected in the agent's salary and yields a competitive advantage over principal-agent relationships using legacy financial systems with expensive auditors.

Transparency is a way of reducing the monitoring cost (Eisenhardt 1985) for a principal when monitoring the behavior of an agent. Because full transparency and thus surveillance is no worthy trade-off silver bullet for reducing corruption, I seek to outline a golden middle way which can be leveraged for the common good. Transparency has lately been seen as a critical factor in reducing dysfunctionalities in countries with an abundance of natural resources (EITI 2019). Thus countries rich in resources have taken several initiatives like the Extractive Industries Transparency Initiative (EITI). The initiative focuses on revenue streams from extractive industries such as minerals and petroleum (EITI 2019).

In organizations which are seen as a nexus of contracts (Eisenhardt 1985) where risk is shared collectively performance can be evaluated through monitoring and rewards performance. Here a country's legal system is vital for how the governance of the firm evolves. If a country requires external auditing of financial information, MHC's immutable and transparent transactions can help reach equilibrium with the governance mechanisms of the state. Thus, as Denis (2001) argues, meaningful relationships between mechanisms, performance, and value can be observed. Using the MHC in organizational contracts reduces the risk of illicit financial operations such as fake receipts increases the whole organizations' financial transparency (Eisenhardt 1985). This makes internal audits easier, and making fake receipts is impossible as the transaction is indistinguishable from the receipt.

The MHC has the capabilities to increase financial transparency because the smart contract transactions provide timely and extremely reliable economic information, which can be made accessible to relevant stakeholders. The financial information provided is concerned, of good quality, and reliable as the transaction and receipt is indistinguishable, accessible as it is openly available on the internet.

Therefore, it is crucial to consider blockchain not exclusively as a financial tool but also a governing tool. Certain conditions can, for example, be put in place for transparently conducting certain transactions. For example, when all transactions are immutably recorded, accounting practices get automated, and the trusted individual doing the accounting is replaced by predictable and immutable software code. This reduces the need for internal government audits and due diligence to find if the accountants are trustworthy because a massive part of their job can be automated.

Using the MHC to increase financial transparency can help reduce corruption Because a lack of transparency can increase corruption in natural resource-rich countries, and empirical evidence suggests that transparency is associated with less corruption (Sohail & Cavill 2008). Transparency is also essential for human development and given blockchain; a tool for transparency in finance; it might also be necessary for social development.

5.2.1 Principal-Agent Relationship & MHC

Given the capabilities of blockchain, and the capabilities of cryptocurrency transactions in smart contracts as s transactional supplement to legal, the principal-agent relationship will be investigated. This section will focus on how using cryptocurrency transactions as an alternative to bank and cash transactions in legal contracts as outlined in 7.1 Minimum Hybrid Contract (MHC) impacts agency theory.

I have chosen four relevant propositions to the principal-agent relationship proposed by Eisenhardt (1989) as a premise for this part of the discussion.

> Proposition I: When the contract between the principal and agent is outcome based, the agent is more likely to behave in the interests of the principal (Eisenhardt 1989).

The smart contract in the MHCs cannot read the state of the world with high reliability and accuracy, incorrect information about a package being delivered can, for example, be given to the smart contract in an MHC to trigger a cryptocurrency transaction. Thus an outcome-based contract will be mostly unaffected by MHCs compared to current legal contract as for now unless the transaction is the goal of the contract itself such as paying back a loan. This is because it is trivial to audit the transaction, and thus, there are low costs of acquiring the information about the outcome in the MHC. Therefore if the outcome is a financial transaction agency costs as in monitoring the agent's actions, information asymmetry and agency costs are reduced.

> Proposition 2: When the principal has information to verify agent behavior, the agent is more likely to behave in the interests of the principal (Eisenhardt 1989).

Considering that transactions in the MHC can be audited instantly and are immutable, all financial actions of agents are transparent to the principal if blockchain is used. For example, an MHC can be used to pool funds a principal gives to an agent to conduct the assigned task(s) and every time the agent spends the funds the principal can receive the financial information. Thus the MHC can be used as a transparency and surveillance mechanism for financial information such as accounting, cost accounting, and budgeting.

> Proposition 3: Information systems are positively related to behavior-based contracts and negatively related to outcome-based contracts (Eisenhardt 1989).

In the context of this thesis, the smart contract in the MHC is an information system for figuring out the state of who owns what money. Thus MHC indicates that behavior-based contracts will

be affected positively, and outcome-based contracts will be less affected unless the financial transaction or audit is the outcome.

> Proposition 4: Outcome uncertainty is positively related to behavior-based contracts and negatively related to outcome-based contracts.

Using the MHC for budgeting and financial surveillance can reduce outcome uncertainty. The financial behaviour of the agent is surveillable and all transactions can be inspected as they are conducting. Thus the outcome becomes more certain for the principal as the financial transactions point in a certain direction and shows what financial actions the agent conducting to reach the goal of the contract in real time. Also behaviour-based contracts can be enhanced if the behaviour is financial.

5.3 Strategy for Regulating Blockchain

This chapter discusses how financial regulators can regulate smart contracts in such a way that the adoption of the MHC is feasible. I will argue that to regulate cryptocurrencies without destroying it, fungibility must be maintained, and it must be treated as money. Having done so, I will discuss how previous financial innovations has been unsuccessfully regulated and cause global systemic havoc, then regulatory lessons from the early days of the internet are presented as feasible options, and finally, regulatory strategies for adopting the MHC are recommended because:

> Financial legislation has never really involved any elements revealing a consistent or logical system of legislation (Tietje & Lehmann 2010).

The MHC is fundamentally challenging to incumbents such as clearinghouses, states issuing fiat currencies and banks as it uses a new form of money; cryptocurrency. The computer and incentive infrastructure being used by financial incumbents relies on decades-old technology and corporate structures. Several financial regulators, such as the Financial Crimes Enforcement Network (FinCEN) and the Internal Revenue Service (IRS) in the United States, are currently

adopting and defining positions related to cryptocurrencies in their regulations. An example is "Coin Center," a cryptocurrency think thank (Valkenburgh 2019), which deems that the latest regulations released by FinCEN (2019) as of the time of writing mostly follow their recommendations. On the other hand, the IRS's current stance on smart contracts is underdeveloped and confusing, and the cryptocurrency experts at Coin Center experts are not sure how to interpret the information.

Current legal frameworks have to adopt if their citizens are to leverage the capabilities of MHCs. Most importantly, the Securities and Exchange Commission (SEC) has recently suggested that the cryptocurrencies Bitcoin and Ethereum can serve as legal tender (Schlegelmilch 2019). Furthermore, US legislators have already begun supplementing contracts with smart contracts. Delaware has adopted legislation authorizing smart contract ledgers for state records and regulatory functions such as tracking liens and corporate shares (Roberts 2017). The state Arizona has instigated a law declaring that blockchain-based digital signatures are legally enforceable (Higgins 2017) and Vermont has declared that blockchain-based evidence is admissible in court (Vermont general assembly 2018). This suggests that blockchain, irrespective of the MHC is transcending being a marginal technology and increasingly becoming an established de facto standard for transferring value over the internet, similar to how the TCP/IP protocol is the de facto standard for transferring information over the internet.

For example, alternative cryptocurrencies claiming to be money are not always accepted by regulators as money. The "Kin" so-claimed cryptocurrency controlled by a private company (Canellis 2019) is as of the time of writing in a dispute with the IRS. Kik, the company behind Kin, is aiming to develop a form of money using cryptocurrency but the IRS holds the position that Kin is not money, but a security. No matter the outcome, regulatory disputes as this stifles development and promotes insecurities as how to proceed and if there will be any legal consequences.

Even if cryptocurrencies are made illegal, they would still work for anyone with access to the internet, and the company Blockstream (2019) has released a satellite relay which gives the capability to conduct a Bitcoin transaction using a satellite antenna. Blockchain has been used for several scams and Ponzi-schemes such as the pyramid scheme "Bitconnect," due to its unregulated nature, which enables an entirely free market (Chohan 2018). More than 80% of all cryptocurrency-based crowdfunding campaigns conducted online in 2017 were outright scams (SATIS Group 2018). Thus even though cryptocurrencies are jurisdiction-neutral, barriers such as laws and regulations can have unintended consequences and halter innovation as a bi-effect, in the end, state regulators have been given the responsibility to intervene in illicit/fraudulent cases and bring justice to criminals to keep order in society.

I am not going to elaborate whether any cryptocurrency is legitimate because the point is that these disputes can undermine the legitimacy of cryptocurrencies in general and stifle experimentation and innovation. Setting barriers for further development can halter the adoption of blockchain technologies in general and delay the time until society can reap the benefits. For example, the Special Secretary of the Federal Revenue of Brazil (RBF 2019), a financial regulator in the country, has issued "Instruction 1888" which passes new rules to come into force on August 1st. Essentially this means that all legal entities, exchanges and individuals carrying out operations using cryptocurrencies have to inform the Brazilian treasury of every detail of their transaction, with the exception of foreign exchanges this an outright 100% transparent policy. This also equals to 100% in domestic cryptocurrency transactions and is domestically a tool for totalitarian surveillance.

Blockchain startups often search for and settle in the legislations most fitting to their business model known as "regulation shopping". The largest cryptocurrency exchange in the world by volume "Binance", which has conducted a strategic regulation shopping move by moving their corporation from Hong Kong to the more cryptocurrency friendly regulation of Malta (Paul 2018). When tax revenues from cryptocurrency exchanges such as Binance are realised, I believe

competition among regulators for bringing the most profitable cryptocurrency companies into their regulation and reaping the tax benefits could occur.

5.3.1 Fungibility

Entrepreneurs become wary when regulators choose to obtain all information about cryptocurrencies and transactions such as what a person owns what cryptocurrency. Having cryptocurrencies accepted as a form of money without destroying its fungibility by making certain units illegal, is favorable for entrepreneurs exploring the blockchain space and societies seeking to leverage blockchain's capabilities. Entrepreneurs have to take a financial risk when choosing to work on a startup. If there is regulatory opposition or uncertainty in addition to the financial risk, the entrepreneur acts risk-adversely and tries to avoid it through regulation shopping and incorporates in the new legislation.

Entrepreneurs become wary when regulators choose to obtain all information about cryptocurrencies and transactions such as what person owns what cryptocurrency. Having cryptocurrencies accepted as a form of money without destroying its fungibility by making certain units illegal, is favourable for entrepreneurs exploring the blockchain space and societies seeking to leverage blockchain's capabilities. Entrepreneurs have to take a financial risk when choosing to work on a startup. If there is regulatory opposition and/or uncertainty in addition to the financial risk, the entrepreneur acts risk-adversely and tries to avoid it through regulation shopping and incorporates in a new legislation.

5.3.2 Financial innovation

The MHC is a financial innovation which is interconnected to the existing legal and regulatory space. Extensive experience with financial innovations as in how new financial products are invented, introduced, and diffused is only one generation old. Both regulators and inventors have low experience with adopting financial innovations which are critical to the health of global economies and markets (Delimiatsis 2011).

The financial crisis in 2008 was caused by rapid innovative developments in global financial services such as over-the-counter derivatives products (Pagano & Volpin 2008). These innovations were used for credit risk modeling causing information asymmetry problems, and the increased complexity of the system made risk assessment harder and therefore, risk management more difficult (Delimiatsis 2011). The dynamic nature of financial innovations can cause their consequences to change over time. This is exemplified in the financial crisis of 2008 when regulators failed to act proactively, neither did they react swiftly in regulating new financial innovations (Marques-Ibanez & Scheicher 2009). Innovative financial products are linked inextricably to global financial markets coordination, financial markets, regulatory cooperation, and one should consider how financial innovations can lead to financial fragility and instability as seen in the financial crisis of 2007-08 (Delimatsis 2011).

Financial innovation is a dynamic, ongoing process entailing the creation and popularization of new financial instruments and technologies, markets, and institutions (Lerner & Tufano 2011). Litan (2010) argues that financial innovation has transformed how finance works. Structural changes, technological advances or new industrial structure in financial sectors has boosted globalization by increasing cross-border trade in financial services (Claessens 2010), and Allen and Gale (1994) argue that financial innovation increases welfare.

Financial innovation is a dynamic, ongoing process entailing the creation and popularization of new financial instruments and technologies, markets and institutions (Lerner & Tufano 2011). Litan (2010) argues that financial innovation has transformed how finance works. Structural changes, technological advances or new industri structure in financial sectors has boosted globalization by increasing cross-border trade in financial services (Claessens 2010), and Allen and Gale (1994) argues that financial innovation increases welfare.

Financial innovation is, in most instances, very much ahead of current regulation (Delimatsis 2011). For example Bitcoin which is the first cryptocurrency was unregulated for many years after it launched, and the MHC would be illegal by default in any of the legislations where

Bitcoin is unlawful such as in Dar al-lifta (2017) which is the primary Islamic legislator in Egypt has classified Bitcoin transactions as "haram" (prohibited under Islamic law), and Algeria where the financial law has prohibited the use of any cryptocurrencies (Journal Officiel 2018). Regulating innovative financial products after the fact is regarded as being counterproductive and a delaying factor for innovation, but regulators prefer to intervene when the side-effects of business innovation have become apparent. In practice agency problems, supervisory forbearance and complex products can delay regulatory intervention and regulatory intervention vis-a-vis the financial innovation can be challenging (Freixas & Parigi 2009).

In the current stage of financial development, it is argued that more is at stake when regulatory intervention affects the pace of financial innovation. When regulators create inflexible and stringent rules, this can be a disincentive for the innovator and stifles the development of innovative financial products. (Delimatsis 2011). Regulation can stifle innovation, and there is evidence that regulator intervention can cause harmful effects on financial innovation (White 1997).

Having a revolutionary change in financial services can cause tremendous systemic risky and be very costly (Tufano 1989), and financial innovation typically happens in evolutionary steps of adopting prior financial products (Tufano 2003).

> Regulation can (...) encourage innovation in globalized financial markets if it seeks to harmonize certain requirements across jurisdictions such as reporting requirements, thereby diminishing compliance costs and facilitating market access (Delimatsis 2011)

The idea sometimes put forward that more regulation may impede innovation may not hold: Better regulation may direct entrepreneurial talents to financial innovations which can enhance societal wellbeing (Delimatsis 2011).

Recent blockchain-based financial innovations similar to the MHC has affected regulation by crossing national borders by default, and in this sense, there is a case for global coordination of

financial regulations to level the playing field. In such cases, enhanced transparency, a central good-governance principle, and sharing information across borders can allow for well-meant regulatory competition and ultimately encourage innovation, while allowing for better supervision and informed investment decisions. In any event, there is a high level of learning-by-doing in this area, and we are at the beginning rather than the end of changes and innovations such as the MHC in the global financial architecture (Delimatsis 2011).

Requiring public disclosure of certain critical financial business information in specific contracts may ultimately have adverse effects and may even reduce market liquidity. Therefore, it seems that disclosure exclusively to the corresponding regulator or supervisory authority would be much more meaningful. Public disclosure can still be required, but perhaps in a later date so that it does not affect business decisions nor allows for misuse of disclosed information (Delimatsis 2011).

5.3.3 The MHC in Context

The MHC architecture described in Chapter 5.1 it leverages the smart contract and leaves the legal contract unchanged, and it handles financial transactions using smart contracts which is a before the fact upgrade to current contracts while leaving after the fact dispute resolution unchanged. After the fact disputes are still left up to legal contracts and institutions to decide and therefore, the MHC will not affect the structure of the legal process, and court processes will remain unchanged.

The illustrative case in Chapter 2.2 shows that business infrastructure in Brazil is in a fragile state, and as the PWC (2017) reports factors for business failure in which I believe the MHC can mitigate. The MHC increases financial transparency and removes the need for excessive legal bureaucracy and formalities for auditing, and the financial information is of better quality than a private bank and cash ledgers because transactions and the receipts in the MHC are indistinguishable. Agents can use previous MHCs to show prospecting principals looking for

new contracts that transactions from previous contracts were successful, and there is not a significant need for restructuring a contract to implement an MHC.

The MHC provides several of the related properties I have selected from what Ball (1995) calls out for in Chapter 2.2 to regain public trust in Brazillian institutions thus it can make the legal contract more trustworthy answering RQ1. The MHC reduces the cost of enforcing financial transactions and auditing in contracts and defines property rights of money using public-private key pairs for addresses and authenticating transactions. Practises for accounting and disclosure become automated and removes potentially corrupt personnel and the capability to tamper with records, and regulators can trust more in market integrity as the financial information they receive about the market is more accurate and cannot be tampered with by corrupt actors.

5.3.4 The MHC and The Legal Status Quo

As an elaboration on designing an MHC to answer RQ2 this section, regulatory strategies for states wishing to implement the MHC is discussed. Financial regulators are recommended to use "safe harbors" where specific activities are excluded from legal enforcement and "regulatory sandboxes," which is similar but regulated in time and scale. Using these strategies regulators can collaborate with actors using MHCs and find a golden middle way which is probably somewhere between not regulating it at all and potentially causing a systemic failure such as outlined in Chapter 5.3.2, and making the smart contract part of the MHC and thus making the MHC itself illegal as is the case in Algeria (Journal Officiel 2017).

A safe harbor is a mechanism to forestall legal enforcement. This mechanism excludes specific activities from legal obligations. In a situation where firms can take sufficient measures to police themselves, a safe harbor incentivizes them to do so and specifies what conduct is necessary. Classic examples of safe harbors in the realm of technological advances are:

1. The 1996 Telecommunications Act § 230: "online services will not be treated as publishers" This means that online publishers are not liable for content created by their users.

2. The 1998 Digital Millennium Copyright act: protects against copyright infringement as long as infringing material was removed from the platform when notified by authorities. (Communications Decency act 1996)

These broadly defined safe harbors from the early days of the public internet make it hard to restrict online activity, which is clearly harmful. The harmful activity includes bullying and harassment because intermediaries have zero incentive to take an active role. On the flip side, these twin safe harbors were a significant factor in the rapid growth of internet-based application in the 1990s. They were essential to spreading user-driven web services and social media. They encourage innovation because services are assured that they are safe from liability for the user-generated content.

To enable adoption of smart contracts in current jurisdictions without the threat of regulatory crackdown legislative safe harbors for blockchain-based services is advocated by blockchain think thank Coin Center (Valkenburgh 2017). Verily in a safe harbor bill named the Blockchain Regulatory Certainty Act, which is at the time of writing being proposed to be accepted into US legislation for the second year in a row. The bill has bipartisan support and could provide room to innovate and integrate smart contracts with current legal frameworks (US Congress 2019).

A regulatory sandbox is similar to a safe harbor but is confined in time or scale, and it suggests an enclosed space for experimentation and play. Regulatory authorities exempt specific companies or activities from regulation to foster startup activity and experimentation. The difference between a sandbox and a safe harbor is that regulatory sandboxes are not necessarily permanent and usually only applies to new firms. Safe harbors are designed to help nascent firms with sparse resources to administer content on their platforms but have ended up helping large tech companies such as Google and Facebook (Werbach 2018)

Therefore regulatory sandboxes are useful because they can be constructed to help organizations at early stages of development and disappear when they mature. Regulatory sandboxes allow

legal regimes to operate more hospitable towards software-directed environments. The Financial Conduct Authority (FCA), which is the primary financial regulator in the United Kingdom, has established a fintech sandbox program for companies to experiment with new services (Financial Conduct Authority 2017). Firms can apply to operate in the sandboxed environment, and if they are approved, they can introduce new services without being obliged to follow specific regulations for a given timeframe. Meanwhile, FCA closely monitors the companies activities and gain a better understanding of new platforms. In the first round of companies being accepted into FCA's regulatory sandbox, the most significant percentage accepted were blockchain-related.

6 Conclusion

In the light of how current contracting practices and legislators globally are all affected by systemic corruption at some level such as in the illustrative case of Operation Car Wash in Brazil in Chapter 2.2, I have developed an architecture for the Minimum Hybrid Contract (MHC). The MHC is a practical and evolutionary step for contracting using smart contracts as supplements to legal agreements for financial transactions. Agency theory, which focused on contractual relationships has been used to discuss the capabilities and implications of the MHC, and finally I have focused on two paths: One strategic path for regulators and innovators and one for how MHCs can affect agency theory issues as it increases information sharing, reduces agency costs and can potentially mitigate moral hazard because the financial transactions in the MHCs and immutable transactions enables more trustworthy and cost-effective auditing.

Using the MHC, depending on and trusting a third-party for financial transactions is no longer needed as trust is no longer placed in individuals and central institutions, but instead distributed across the user base. Questionable central authorities are replaced by communities of peers in the form of peer-to-peer networks. No single entity can take unilateral actions on behalf of the community, as has been the case with the Trump Administration's unilateral decision to ban international trade with Iran by blocking Iranian access to the Society for Worldwide Interbank

Financial Telecommunication (SWIFT) network. This prevents the countries banks from using SWIFT, which is the international standard to conduct financial transactions without any basis in international law or customs. In the democratized context offered by smart contracts, corporations and states cannot unilaterally defy the community and break the rules of the system; thereby the MHC can create a more trustworthy system (Sun et al. 2016; Scotts & Zachariadis 2012).

Chapter 5.2 shows that the MHC affects information asymmetries, moral hazard, and agency costs in agency theory. In light of the MHC, agency theory is most affected by its transparent and immutable properties. Eased sharing and increased transparency of financial information lower the cost of sharing information and decreases information asymmetries. Thus the agency cost called monitoring cost of the principal is reduced as the price of acquiring financial information is reduced. The MHC provides a similar trusted network as Razavi and Iverson (2006) calls out for in supply chains to exchange interpersonal information, but specifically for financial information. Moral hazard is decreased as the MHC provides a deterrent against financial crime, given the transparent and immutable properties of its business transactions.

Chapter 5.3 on blockchain regulation strategy to outlines a regulatory pathway for smart contracts in such a way that adoption of the MHC is feasible. If smart contracts are made illegal such as in Algeria the MHC cannot use a smart contract as a supplement to a legal contract, and innovators building MHCs will probably incorporate in a different country as in the case of the currently largest cryptocurrency exchange by volume: Binance, which moved its business from Hong Kong to Malta due to legislative reasons (Paul 2018).

Financial legislators have never managed to create a consistent or logical legislation system, as discussed in Chapter 5.3, and most importantly, regulators must maintain fungibility of the cryptocurrency used in the MHC. To find a golden middle way for the development of regulation without stifling innovation, regulators are recommended to learn from the regulatory strategies used during the emergence of the internet in the late 1990s. To avoid financial turmoil and reap

the tax returns from innovators succeeding in building large businesses in their legislation, regulators should implement safe harbors where specific activities are excluded from legal obligations, and regulatory sandboxes where regulatory slack is given in limited time and scale should also be performed.

To utilize the MHC for societal wellbeing finding a golden middle way between private and transparent transactions is essential, and a balance must be struck between transparency and the basic human need for privacy and secrets (Harari 2014). Satoshi Nakamoto (2008) has invented a way to conduct open, borderless, censorship-resistant, and neutral transactions without having to trust any corruptible central authority is a game-changer for making contracts more trustworthy (**RQ1**), and will most definitely affect all of finance. As seen in Chapter 5 smart contracts has the capability to disrupt more than just the financial part of a contract (Werbach 2018), using blockchain for after the fact dispute resolution is already being pioneered by the blockchain project augur, showing that governance and contracting might end up relying entirely on online blockchain-based courts (**RQ2**) as opposed to current legal courts currently run by states and organizations such as the European Union. since blockchain transactions are transparent, with immutable properties, it is also more trustworthy and makes auditing more cost-effective. Ultimately it succeeds in mitigating moral hazard, information asymmetries and agency costs emphasises by agency theory.

References

Abel A. & Bernanke B. (2005). Macroeconomics (5th ed.). New Jersey, United States: Pearson. pp. 522–532.

Adams, M. B. (1994). Agency Theory and the Internal Audit. Managerial Auditing Journal, 9(8), pp. 8–12. doi:10.1108/02686909410071133

Adler D. (2018) Silk Road: The Dark Side of Cryptocurrency. Fordham Journal of Corporate Financial Law. [online] Available at: https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/ [Read 23.05.2019]

Ahmad, I. U., Russell, J. S., and Abou-Zeid, A. (1995). "Information technology (IT) and integration in the construction industry." Constr. Manage. Econ., 13(2), 163–171.

Allen F. and Gale D (1994) Financial Innovation and Risk Sharing. MIT Press

Anderson C. W. (1999) Financial contracting under extreme uncertainty: an analysis of Brazilian corporate debentures. Journal of Financial Economics issue 51 pp.45—84

Ante L. & Fiedler I. (2019) "Cheap Signals in Security Token Offerings," Blockchain Research Lab. [online] Available at: https://www.researchgate.net/publication/331287045_Cheap_Signals_in_Security_Token_Offerings [Accessed 05.05.2019]

Arrow, K. (1962) 'Economic welfare and the allocation of resources for invention', in K. Arrow (ed.) The Rate and Direction of Invention Activity: Economic and Social Factors: A Report of the National Bureau of Economic Research, Princeton, NJ: Princeton University Press, pp. 609–25.

Arrow K. (1971) Essays in the Theory of Risk-Bearing. Amsterdam:North-Holland Publishing Company.

Arajo J. F. F. E, Tejedo-Romero F. (2016) Local government transparency index: determinants of municipalities' rankings. International Journal of Public Sector Management, 29(4), 327–347. doi:10.1108/ijpsm-11-2015-0199

Aslam N. (2018) Banks Banning Cryptocurrency Purchase On Credit Cards, Why? Forbes. [online] Available at: https://www.forbes.com/sites/naeemaslam/2018/02/05/banks-banning-cryptocurrency-purchase-on-credit-cards-why/#6d73d4783cf9 [read 23.05.2019]

Ball, R., (1995). Making accounting more international: why, how, and how far will it go? Journal of Applied Corporate Finance 8, pp. 19—29.

Bellver A. & Kaufmann D. (2005) 'Transparenting Transparency' Initial Empirics and Policy Applications. The World Bank

Ben-Sasson E., Chiesa A., Garman C., Green M., Miers I., Tromer E., Virza M. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. [online] Available at: http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf [Accessed 03.03.2019].

Bitcoinuptime.com (2019) Bitcoin-uptime. [online] Available at: Bitcoinuptime.com [Accessed 12.03.2019]

Bitcoin.org (2019). Choose your Bitcoin wallet. [online] Available at: https://Bitcoin.org/en/choose-your-wallet [Accessed 14.05.2019].

Blockstream (2019) Blockstream satellite. [online] Available at: https://blockstream.com/satellite/ [read 09.06.2019]

Blockchaintechnologies.com (2016). The ultimate guide to blockchain smart contracts. Available at: http://www.blockchaintechnologies.com/blockchain-smart-contracts [Accessed 14.05.2019].

Bowen, P. A., Akintoye, A., Pearl, R., and Edwards, P. J. (2007). "Ethical behaviour in the South African construction industry." Constr. Manage. Econ., 25(6), 631–648.

Brunetti, A., & Weder, B. (2003). A free press is bad news for corruption. Journal of Public Economics, 87, 1801–1824.

Buterin V. (2013) "Ethereum White Paper", [online] Available at: https://github.com/ethereum/wiki/wiki/White-Paper [Accessed 05.05.2019]

Canellis D (2019) Kik raised $98M with a potentially illegal ICO. Now it wants your money to fight the SEC. Coindesk [online] Available at: https://www.coindesk.com/sec-negotiations-have-cost-kik-5-million-says-ceo [read 29.05.2019]

Castillo M. (2019) "Customers Can Spend Bitcoin At Starbucks, Nordstrom And Whole Foods, Whether They Like It Or Not". Forbes [online] Available at: https://www.forbes.com/sites/michaeldelcastillo/2019/05/13/starbucks-nordstrom-and-whole-foods-now-accept-Bitcoin-just-dont-ask-them/#35cff98d2252 [accessed 28.05.2019]

Chaia A., Dalal A., Goland T., Gonzalez M. J., Murduch J. & Schiff R. (2009) Half the World is Unbanked. McKinsey & Company. [online] Available at: https://www.mckinsey.com/industries/social-sector/our-insights/half-the-world-is-unbanked [read 27.05.2019]

Carnevale, D.G. (1995). TRUSTWORTHY GOVERNMENT: LEADERSHIP AND MANAGEMENT STRATEGIES FOR BUILDING TRUST AND HIGH PERFORMANCE. San Francisco: Jossey-Bass

Chohan U. W (2018) Bitconnect and Cryptocurrency Accountability. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3131512 [read 05.06.2019]

Claessens S. 2003 'Regulatory Reform and Trade Liberalization in Financial Services', in A. Mattoo and P. Sauvé (eds), Domestic Regulation and Service Trade Liberalization (Oxford University Press).

Claus I. and Kim K. (2004) Agency costs and asymmetric information in a small open economy. Econometric Society 2004 Far Eastern Meetings 787, Econometric Society.

Communications Decency act (1996), Pub. L. No. 104-104, § 502, 100 Stat. 133, 134-35 (codified as amended at 47 U.S.C. § 223(2012)); Pub. L. No. 105-304, § 202, 112 Stat. 2860, 2877-78 (codified as amended at 17 U.S.C. § 512(2012)

Crosby, M. (2016). "BlockChain Technology: Beyond Bitcoin. Pantas and Ting Sutardja Center for Entrepreneurship and Technology Berkeley Engineering no. 2: 16.

da Costa, R. T., (1993). Preface. In: Tertuliano, F., Pessoa, I., Francisco de Aguiar, J., Ayoub, R., Trancanella, R., Rioli, V. (Ed's.), Full Disclosure: como Aperfeiçoar o Relacionamento das Empresas Abertas com o Mercado de Capitais. Editora Maltese, São Paulo.

Dar al-lifta (2017) Religious Decree No. 4205, The Status of Transactions in Bitcoins and other Cryptocurrencies under Islamic Law, EGYPT'S DAR AL-IFTA. [online] Available at: http://www.dar-alifta.org/ar/ViewFatwa.aspx?sec=fatwa&ID=14139 archived at https://perma.cc/432D-NHE5 [read 09.06.2019]

Dash (2019) Your money, your way. [online] Available at: https://www.dash.org [read 09.06.2019]

Delimatsis P. (2011) Financial Innovation and Transparency in Turbulent Times TILEC Discussion Paper No. 2011-031. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1865747 [read 04.06.2019]

Deloitte (2016) Tech Trends 2016 Innovating in the digital era, Blockchain: Democratized trust. Available at: https://documents.dupress.deloitte.com/TechTrends2016 [Read: 04.04.2019]

Demski, J.. & Feitham, G. (1978) Economic incentives in budgetary control systems. Accounting fleview, 53, 336-359.

Denis D. K. (2001) Twenty-five years of corporate governance research … and counting. Review of Financial Economics 10: 191–212

Department of Justice (2014) Second Vice President of Equatorial Guinea Agrees to Relinquish More Than $30 Million of Assets Purchased with Corruption Proceeds. [online] Available at: https://www.justice.gov/opa/pr/second-vice-president-equatorial-guinea-agrees-relinquish-more-30-million-assets-purchased [read 03.06.2019]

Douceur J. (2002), The Sybil Attack, IPTPS '01 Revised Papers from the First International Workshop on Peer-to-Peer Systems 251. [online] Available at: http://nakamotoinstitute.org/static/docs/the-sybil-attack.pdf [Accessed 17.3.2019]

Economica (1931). The 'Paradox' of Saving. Economica. 32.

Eichengreen B. & Temin P. (2000). The Gold Standard and the Great Depression. Contemporary European History, 9(2). pp. 183-207.

Edelman (2017) Edelman trust barometer 2017. [online] Available at: https://www.edelman.com/trust2017/ [read 03.03.2019]

Edelman (2019) Edelman Trust Barometer Global Report. [online] Available at: https://www.edelman.com/sites/g/files/aatuss191/files/2019-02/2019_Edelman_Trust_Barometer_Global_Report.pdf [Accessed 03.06.2019]

EITI (2019) Extractive Industries Transparency Initiative. [online] Available at: https://eiti.org/ [Accessed 22.05.2019]

Eisenhardt K. M. (1985) Control: organization and economic approaches. Management science Vol. 31 No. 2.

Eisenhardt, K.M.. (1989). Agency Theory: An Assessment and Review. The Academy of Management Review, 14(1), Retrieved from https://www.jstor.org/stable/258191

Eris:Legal (2014) "Putting The Contracts in Smart Contracts", Eris industries. [online] Available at: https://www.erisindustries.com/components/erislegal.html [Accessed 12.05.2019]

Ethereum Classic (2017). ethereum classic. [online] Available at: https://ethereumclassic.org/ [Accessed 14.05.2019].

EthHub (2019) "Ethereum 2.0 (Serenity) Phases" [online] Available at: https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/eth-2.0-phases [Accessed 03.03.2019]

Financial Conduct Authority (2017) "financial conduct authority provides update on regulatory sandbox" The Financial Conduct Authority. [online] Available at: https://www.fca.org.uk/news/press-releases/financial-conduct-authority-provides-update-regulatory-sandbox [Accessed 12.05.2019]

FinCen (2019) Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies. Financial Crimes Enforcement Network (FinCen) [online] Available at: https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20CVC%20Guidance%20FINAL.pdf [read 29.05.2019]

Federalreserve.gov (2009). Federal reserve statistical release. Archived June 5, 2009, at the Wayback Machine. [online] Available at: https://web.archive.org/web/20090605101615/http://www.federalreserve.gov/releases/h6/hist/h6hist1.htm [Accessed 14.05.2019].

Ferrara, P. (2013). Rethinking Money: The Rise Of Hayek's Private Competing Currencies. [online] Available at: https://www.forbes.com/sites/peterferrara/2013/03/01/rethinking-money-the-rise-of-hayeks-private-competing-currencies/#76d74ba83bab [Accessed 14.05.2019].

Figueiredo F. O. (2016) "Inside the Car Wash: The Narrative of a Corruption Scandal in Brazil". [online] Available at: https://www.psa.ac.uk/sites/default/files/conference/papers/2016/Car%20Wash%20PSA%20final1_0.pdf [Accessed 14.05.2019]

Foreign Policy (2009) The 2009 Failed States Index. [online] Available at: https://foreignpolicy.com/2009/06/21/the-2009-failed-states-index [Accessed 20.05.2019]

Freixas X. and Parigi B. (2009) 'Rules vs. discretion in times of financial innovation', paper presented at a conference on 'Internationalization of Services: Competition and Regulatory Interaction in Europe', pp. 25-27 June,

GAN (2019) Compliance Guides. Business Anti-Corruption Portal. Available at: https://www.business-anti-corruption.com/compliance-quick-guides/brazil/

Geiregat S. (2018). Cryptocurrencies are (smart) contracts. Computer Law & Security Review. Volume 34, Issue 5, pp. 1144-1149

Global Witness (2018) "Global Witness reveals Brazil's Car Wash corruption scandal may have cost the country eight times more than the £1.4 billion stolen"[online] Available at: https://www.globalwitness.org/en/press-releases/global-witness-reveals-brazils-car-wash-corruption-scandal-may-have-cost-country-eight-times-more-14-billion-stolen/ [Accessed 14.05.2019]

Golembiewski R,.T .(1979). Approaches to planned change: Macro-level interventions and change agent strategy. New York: Marcel Dekker.

Graeber D. (2001). Toward an anthropological theory of value: the false coin of our own dreams. Basingstoke, United Kingdom: Palgrave Macmillan. pp. 153–154.

Graeber D. (2011). Debt: The First 5000 Years. New York: Melville House Publishing.

Grigg I. (2004) "The Ricardian Contract." Accessed March 13, 2019. [online] Available at: http://iang.org/papers/ricardian_contract.html [Accessed 12.05.2019]

Harari Y. (2014). Sapiens: A Brief History of Humankind. London: Harvill Secker.

Harris, M., & Raviv, A. (1978) Some results on incentive contracts with application to education and employment, health insurance, and law enforcement. American Economic Review. 68, 20-30.

Hayne K. M. (2017) GOVERNMENT CONTRACTS AND PUBLIC LAW. Melbourne Law School, The University of Melbourne. [online] Available at: https://law.unimelb.edu.au/__data/assets/pdf_file/0004/2494336/05-Hayne.pdf [read 04.06.2019]

Hennart, J-F. (1989) 'Can the "new forms of investment" substitute for the "old forms?" A transaction cost perspective', Journal of International

Hendrik S. & Mochalski K. (2009). "Internet Study 2008/2009" (PDF). Leipzig, Germany: ipoque. Archived from the original (PDF) on 1 April 2014. Retrieved 3 October 2011. "Peer-to-peer file sharing (P2P) still generates by far the most traffic in all monitored regions – ranging from 43% in Northern Africa to 70% Eastern Europe."

Henry T. C. Hu (2015), Financial Innovation and Governance Mechanisms: The Evolution of Decoupling and Transparency, 70 Business Lawyer pp.347- 405, available at http://ssrn.com/abstract=2588052

Henry D. & Irrera A. (2017) JPMorgan's Dimon says Bitcoin 'is a fraud'. Reuters [online] Available at: https://www.reuters.com/article/legal-us-usa-banks-conference-jpmorgan/jpmorgans-dimon-says-Bitcoin-is-a-fraud-idUSKCN1BN2PN [read 23.05.2019]

Heuvel, G. V. D. (2005). "The parliamentary enquiry on fraud in the Dutch construction industry collusion as concept between corruption and state-corporate crime." Crime Law Social Change, 44(2), 133–151.

Higgins S. (2017) "Arizona Governor Signs Blockchain Bill Into Law". Coindesk. [online] Available at: https://www.coindesk.com/arizona-governor-signs-blockchain-bill-law [Accessed 05.05.2019]

Hoepman J. (2007). Distributed Double Spending Prevention⋆. [online] Available at: https://arxiv.org/pdf/0802.0832.pdf [Accessed 05.02.2019].

Holmes O. W. Jr., (1881). The Common Law (1 ed.). London: Macmillan.

Holström (1979) Moral hazard and observability. The Bell Journal of Economics, Vol. 10, No. 1 pp. 74-91

Macneil I. R. (1978) "Contracts: Adjustment of Long-Term Economic Relations Under Classical, Neoclassical, and Relational Contract Law," Northwestern University Law Review 72 (854)

Ipsey R. (1975). An introduction to positive economics. London, United Kingdom: Weidenfeld & Nicolson. 4th ed. pp. 683–702.

Islam, R (2003), Do more transparent Governments govern better?, Policy Research Working Paper 3077, World Bank.

Jensen C. M. & Meckling H. W. (1976) Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics 3 305-360

Journal Officiel (2018) DE LA REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE. [online] Available at: https://www.joradp.dz/FTP/jo-francais/2017/F2017076.pdf [read 11.06.2019]

JP Morgan (2019a) The Blockchain Center of Excellence. [online] Available at: https://www.jpmorgan.com/global/blockchain [read 23.05.2019]

Kagan R. A. (2009) "Adversarial Legalism: The American Way of Law". Cambridge, MA: Harvard University Press

Kannan, V. & Tan, K. (2006) Buyer-supplier relationships: the impact of supplier selection and buyer-supplier engagement on relationship and firm performance. International Journal of Physical Distribution & Logistics

Kaplan, S.N. and D. Reishus. (1990), 'Outside Directors and Corporate Performance', Journal of Financial Economics 27 (2), pp. 389-410.

Kenny, C. (2009). "Transport construction, corruption and developing countries." Transp. Rev., 29(1), 21–41.

Kiyotaki N. & Wright R. (1991). A Contribution to the Pure Theory of Money. Journal of economic theory. 53. pp. 215-235.

Kolstad I. & Arne W. (2009) Is Transparency the Key to Reducing Corruption in Resource-Rich Countries?. World Development Vol. 37, No. 3, pp. 521–532

KYC360 (2016) Special Report: FAILURES IN ANTI-MONEY LAUNDERING CONTROLS: PAYING THE PRICE. [online] Available at: https://www.riskscreen.com/kyc360/special-report/failures-in-anti-money-laundering-controls-paying-the-price/ [read 03.06.2019]

Lambert, D. & Cooper, M. (2000) Issues in supply chain management. Industrial Marketing Management, 29(1), pp. 65-83.

Lau, H. & Lee, W.B. (2000) On a responsive supply chain information system. International Journal of Physical Distribution & Logistics Management, 30(7/8), pp. 598-610.

Leatherwood, M., & Conlon, E. (1987) Diffusibility of blame: Effects on persistence in a project. Academy of Management Journal 30, 836-848.

Lei No. 12.846, de 1 de Agosto de 2013, Diario Oficial da Uniao [D.O.U] de 2.8.2013 (Braz.) [online] Available at: https://www2.camara.leg.br/legin/fed/lei/2013/lei-12846-1-agosto-2013-776664-publicacaooriginal-140647-pl.html [Accessed 23.05.2019]

Lerner J. and Tufano P. (2011) 'The Consequences of Financial Innovation: A Counterfactual Research Agenda', NBER Working Paper No 16780, February 2011, p. 6.

Lin I, & Liao T (2017) International Journal of Network Security, Vol.19, No.5, PP.653-659. (DOI: 10.6633/IJNS.201709.19(5).01)

Litan R. (2010)'In Defense of Much, But Not All, Financial Innovation', Brookings Institution, February, pp. 2.

Litecoin.org (2019). GLOBAL DECENTRALIZED CURRENCY [online] Available at: https://litecoin.org/ [Accessed 12.03.2019].

Lombrozo E. (2017). Forks, Signaling, and Activation. [online] Available at: https://medium.com/@elombrozo/forks-signaling-and-activation-d60b6abda49a [Accessed 12.03.2019].

Malhotra D., Murnighan K. (2002) "The Effects of Contracts on Interpersonal Trust", Administrative Science Quarterly 47, no. 3 pp. 534-559

Mankiw G. (2007). Macroeconomics. 6th ed. New York: Worth Publishers. pp. 22–32.

Mankiw G. (2014). Principles of Economics. Boston, Massachusetts, United States: Cengage Learning pp. 220.

Marie H. (2019) Us Rep Sherman Calls for Crypto Ban, Says It Threatens to Diminish American Power. Cointelegraph. [online] Available at: https://cointelegraph.com/news/us-rep-sherman-calls-for-crypto-ban-says-it-threatens-to-diminish-american-power [read 23.05.2019]

Marques-Ibanez D. and Scheicher M. (2009) 'Securitization – Instruments and Implications'. The Oxford Handbook of Banking (Oxford University Press, 2010), pp. 488.

Mason-Jones, R. & Towill, D. (1997) Information enrichment: designing the supply chain for competitive advantage. Supply Chain Management, 2(4), pp. 137-48.

Mattereum (2019) Mattereum: Decentralized Digital Twins for Trade, Law and Finance. [online] Available at: https://mattereum.com/ [Accessed 23.05.2019]

Mattoo A. and Subramanian A. (2009) 'From Doha to the Next Bretton Woods – A New Multilateral Trade Agenda' 88:1 Foreign Affairs 15.

McColgan P. (2001) Agency theory and corporate governance: a review of the literature from a UK perspective. Department of Accounting & Finance, University of Strathclyde Draft 22. May 2001.

McFarlane C., Beer M., Brown J. and Prendergast N. (2017). Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1.1. [online] Available at: https://www.patientory.com/wp-content/uploads/2017/04/Patientory_Whitepaper-1.pdf [Accessed 19.04.2019].

Mehlum, H., Moene, K., & Torvik, R. (2006). Institutions and the resource curse. The Economic Journal, 116, pp. 1–20.
Melo A. M. (2016) Crisis and Integrity in Brazil. Journal of Democracy, Volume 27, Number 2, April 2016, pp. 50-65 (Article)

Menezes A. J., van Oorschot P. C. and Vanstone S. A. (1996). "Handbook of Applied Cryptography", CRC Press. [Accessed 05.05.2019] Available at: http://cacr.uwaterloo.ca/hac/

Milne R. & Winter D. (2018) "Danske: anatomy of a money laundering scandal", Financial Times [online] Available at: https://www.ft.com/content/519ad6ae-bcd8-11e8-94b2-17176fbf93f5 [Accessed 14.05.2019]

Miller M. H. (1992) Financial Innovation: Achievements and Prospects, J. APPLIED CORP. FIN., Winter 1992 at 4, 6 n.6..

Monero (2019) MONERO Private Digital Currency. [online] Available at: https://www.getmonero.org [read 09.06.2019]

Mulder L., Dijk E. V., Cremer D. D and Wilke H. A. M (2006) "Undermining Trust and Cooperation: The Paradox of Sanctioning System in Social Dilemmas". Journal of Experimental Social Psychology 42 pp. 147-162.

Mundell R. (2002), The Birth of Coinage. [online] Available at: https://academiccommons.columbia.edu/catalog/ac:114141 [Accessed 14.05.2019].

Nakamoto S. (2008). "Bitcoin A Peer-to-Peer Electronic Cash System." [online] Available at: https://Bitcoin.org/Bitcoin.pdf [Accessed March 6, 2019].

New York Times (2018) "Ex-President 'Lula' of Brazil Surrenders to Serve 12-Year Jail Term". [online] Available at: https://www.nytimes.com/2018/04/07/world/americas/brazil-lula-surrenders-luiz-inacio-lula-da-silva-.html [Accessed 20.05.2019]

North D. (1990) "Institutions, Institutional Change and Economic Performance." Cambridge University Press, Cambridge

Nxt (2014). Nxt whitepaper, created by the Nxt community. [online] Available at: https://nxtwiki.org/wiki/Whitepaper:Nxt [Accessed 03.03.2019]

OECD (2002), Foreign Direct Investment for Development- Maximising Benefits, Minimising Costs, OECD Secretariat.

Oliver D Hart (1988) "Incomplete contracts and the theory of the firm," Journal of Law, Economics, and Organization 4 : 119, 123.

Obermayer B and Obermaier F. (2016) THE PANAMA PAPERS Breaking the Story of How the Rich & Powerful Hide Their Money. Oneworld Publications, London.

OpenLaw (2017) "Introducing OpenLaw", [online] Available at: https://media.consensys.net/introducing-openlaw-7a2ea410138b [Accessed 12.05.2019]

Orre A. & Mathisen H. W (2008) Corruption in fragile states. The Danish Institute for International Studies. [online] Available at: https://www.cmi.no/publications/file/3235-corruption-in-fragile-states.pdf [accessed 20.05.2019]

O'Sullivan A. & Sheffrin S. (2003). Economics: Principles in action. Upper Saddle River, New Jersey: Pearson Prentice Hall. pp. 246.

Ouchi, W, "A Conceptual Framework for the Design of Organization Control Mechanisms," Management Sci., 25 (September 1979), pp. 833-848.

Oxforddictionaries.com (2005). Definition of cryptocurrency in English. [online] Available at: https://en.oxforddictionaries.com/definition/cryptocurrency [Accessed 14.05.2019].

Oxforddictionaries.com (2019) Definition of contract in English. [online] Available at: https://en.oxforddictionaries.com/definition/contract [Accessed 08.06.2019].

Pagano M. Volpin P (2008) 'Securitization, Transparency and Liquidity', CEPR Discussion Paper No DP7105

Paul A. (2018) Binance Moving to Malta. Coin Central [online] Available at: https://coincentral.com/binance-moving-to-malta/ [read 29.05.2019]

Pereira da Silva, J., (1990). Ana´lise Financeira das Empresas. Editora Atlas, São Paulo. , pp. 30—31

Plato (348 BC) The Laws, Book 11, §23, Contracts.

Popov S. (2016). A Probabilistic Analysis of the Nxt Forging Algorithm. Ledger Journal. 1: 69–83. ISSN 2379-5980. doi:10.5195/LEDGER.2016.46. [Accessed 03.03.2019].

Pratt, J.W., Zeckhauser, R. (Eds.), 1985. Principals and Agents. The Structure of Business. Harvard Business School Press, Boston, MA.

PWC (2017) Doing Deals in Brazil.

Razavi M., Iverson L. (2006) Grounded theory of information sharing behavior in a personal learning space, Proceedings of the ACM CSCW '06 Conference on Computer Supported Cooperative Work, pp. 459-468.

Redman J. (2017) After the Boss Calls Bitcoin a 'Fraud' — JP Morgan Buys the Dip. [online] Available at: https://news.Bitcoin.com/after-the-boss-calls-Bitcoin-a-fraud-jp-morgan-buys-the-dip/ [read 06.06.2019]

Reid K., (2013) Banknotes and Their Vindication in Eighteenth-Century Scotland. David Fox and Wolfgang Ernst (eds), Money in the Western Legal Tradition (Oxford University Press, 2014, Forthcoming); Edinburgh School of Law Research Paper No. 2013/19. Available at SSRN: https://ssrn.com/abstract=2260952 or http://dx.doi.org/10.2139/ssrn.2260952

Reinikka, R., & Svensoon, J. (2005). Fighting corruption to improve schooling: Evidence from a newspaper campaign in Uganda. Journal of the European Economic Association, 2(2–3), 1–9.

Reutzel B. (2016) "BNP Paribas Works With Blockchain Startup to Open Source Law" [online] Available at: https://www.coindesk.com/commonaccord-legal-smart-contracts-prove-beneficial-one-bank-veritcal [Accessed: 12.05.2019]

Rizzo P. (2016) "How Barclays Used R3's Tech to Build a Smart Contracts Prototype." Coindesk. [online] Available at: https://www.coindesk.com/barclays-smart-contracts-templates-demo-r3-corda [Accessed 12.05.2019]

Roberts J. J. (2017) "Companies Can Put Shareholders on a Blockchain Starting Today", Fortune [online] Available at: http://fortune.com/2017/08/03/blockchain-shareholders-law/ [Accessed 11.05.2019]

Robinson, J. A., Torvik, R., & Verdier, T. (2006). Political foundations of the resource curse. Journal of Development Economics, 79, 447– 468.

Ross S. (1973). 'The economic theory of agency: the principal's problem'. American Economic Review, 63,134-9.

Ross, M.L., (2001). Does Oil Hinder Democracy? World politics, 53(03), pp.325–361.

Schlegelmilch S. J. and Mendel D. S (2019) U.S. SECURITIES AND EXCHANGE COMMISSION, UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK. Case 1:19-cv-05244 [online] Available at: https://www.sec.gov/litigation/complaints/2019/comp-pr2019-87.pdf [read 08.06.2019]

Sitkin, S. (1987) Secrecy in organizations: The limits of legitimate information control Working paper. University of Texas, Austin.

Silva, A.H.C. & Cardozo, J.S.S. (2012) 'Teoria dos Escândalos Corporativos: Uma Análise Comparativa de Casos Brasileiros e Norte-americanos', Revista de Contabilidade do Mestrado em Ciências Contábeis da UERJ, jan./abr, Vol. 17, No. 1, pp.105–108, Rio de Janeiro.

Silvia C. and Colauto R. D. (2016) Voluntary disclosure in the context of convergence with International Accounting Standards in Brazil. Review of Business Management, [S.l.], v.18, n.62, pp. 658-677.. ISSN 1983-0807

Socolofsky T. and Kale C. (1991) A TCP/IP Tutorial. [online] Available at: https://tools.ietf.org/html/rfc1180 [read 10.06.2019]

Stallings, W. (1990). Cryptography and Network Security: Principles and Practice. Prentice Hall. p. 165. ISBN 9780138690175.

Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

Szabo N. (1996) "Smart Contracts: Building Blocks for Digital Markets" [online] Available at: www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html [Accessed 05.05.2019]

Szabo N. (1997) "Formalizing and Securing Relationships on Public Networks," [online] Available at: https://journals.uic.edu/ojs/index.php/fm/article/view/548 [Accessed 05.05.2019]

Shankman, N.A.(1999), "Reforming the debate between agency theory and stakeholder's theories of the firm." Journal of Business Ethics, Vol. 19, p. 319-334.

Smith A. (1937) The Wealth of Nations, Cannan Edition. Modern Library, New York 1937 pp. 70

Sohail, M., and Cavill, S. (2008). "Accountability to prevent corruption in construction projects." J. Constr. Eng. Manage., 10.1061/(ASCE)0733-9364(2008)134:9(729), 729–738.

Stacher D. (2018) Regulation of Initial Coin Offering (ICO). Chair of Economic Theory Universität Basel. [online] Available at: https://wwz.unibas.ch/fileadmin/user_upload/wwz/00_Professuren/Berentsen_Wirtschaftstheorie/Lecture_Material/Master_s_Thesis/Completed_Master_s_Theses/Master_Thesis_David_Stacher.pdf [read 03.06.2019]

Stank, T., Crum, M. & Arango, M. (1999) Benefits of inter-firm coordination in food industry supply chains. Journal of Business Logistics, 20(2), pp. 21-41.

SATIS Group (2018) Cryptoasset Market Coverage Initiation: Network Creation. [online] Available at: https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ [read 05.06.2019]

Stiglitz, J. E. (1999), "On Liberty, the Right to Know and Public Disclosure: The Role of Transparency in Public Life", Oxford Amnesty Lecture.

Suphachalasai, S. (2005). Bureaucratic corruption and mass media. Environmental economy and policy research discussion paper series. Cambridge: University of Cambridge.

Tapscott D. & Tapscott A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. New York: Penguin Random House LLC.

Takashi D. (2018) IBM and Maersk launch blockchain to reduce shipping time and costs. [online] https://venturebeat.com/2018/08/09/ibm-and-maersk-launch-blockchain-to-reduce-shipping-time-and-costs/ [read 08.06.2019]

The Royal Mint (2019) Legal Tender Guidelines. [online] Available at: https://www.royalmint.com/aboutus/policies-and-guidelines/legal-tender-guidelines [read 28.05.2019]

The World Bank and the United Nations Office of Drugs and Crimes (UNODC) (2010) Stolen Asset Recovery: Toward a Global Architecture for Asset Recovery [online] Available at: https://star.worldbank.org/sites/star/files/GlobalArchitectureFinalwithCover.pdf [Accessed 20.05.2019]

Tietje Cf. C. and Lehmann M. (2010) 'The Role and Prospects of International Law in Financial Regulation and Supervision' 13:3 Journal of International Economic Law 663, pp. 665.

Towill, D. (1997) The seamless supply chain: the predator's strategic advantage. International Journal of Technology Management, 13(1), pp. 37-56.

Trachtman Cf. J.(2010) 'The International law of Financial Crisis: Spillovers, Subsidiarity, Fragmentation and Cooperation' 13:3 Journal of International Economic Law 719, pp. 729

Transparency International (2007) "Corruption risk analysis in Southern Africa," [online] Available at: http://www.transparency.org/news_room/in_focus/2007/nis_africa [Accessed 03.02.2019]

Tobin A. & Reed D. (2017) "The Inevitable Rise of Self-Sovereign Identity," Sovrin Foundation. https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf [Accessed 04.05.2019]

Tufano P. (1989) 'Financial Innovation and First Mover Advantages'. 25th Journal of Financial Economics pp. 213.

Tufano P. (2003), 'Financial Innovation' in G. Constantinides; M. Harris; and R. Stulz (eds), The Handbook of the Economics of Finance, Volume 1A: Corporate Finance (Elsevier).

Uport (2017) "First official registration of a Zug citizen on Ethereum". https://medium.com/uport/first-official-registration-of-a-zug-citizen-on-ethereum-3554b5c2c238 [Accessed 04.05.2019]

US Congress (2019) "H.R.528 - Blockchain Regulatory Certainty Act," 116th Congress, [online] Available at https://www.congress.gov/bill/116th-congress/house-bill/528/all-actions?q=%7B"search"%3A%5B"Hr+528"%5D%7D&s=1&r=1 [Accessed 12.05.2019

Vermont general assembly (2018) "The Vermont Statutes Online", [online] Available at: https://legislature.vermont.gov/statutes/section/12/081/01913 [Accessed 11.05.2019]

Valkenburgh P. V. (2017) "Congress should create a blockchain technology safe harbor. Luckily they already figured it out in the '90s." Coin Center. [online] Available at: https://coincenter.org/entry/congress-should-create-a-blockchain-technology-safe-harbor-luckily-they-already-figured-it-out-in-the-90s [Accessed 12.05.2019]

Valkenburgh P. V. (2019) FinCEN's new cryptocurrency guidance matches Coin Center recommendations. Coin Center [online] Available at: https://coincenter.org/entry/fincen-s-new-cryptocurrency-guidance-matches-coin-center-recommendations [read 29.05.2019]
von Hayek, F. (1977). Denationalization of Money: An Analysis of the Theory and Practice of Concurrent Currencies. London: Institute of Economic Affairs .

Vee, C., and Skitmore, M. (2003). "Professional ethics in the construction industry." Eng. Constr. Archit. Manage., 10(2), 117–127.

Vishwanath, T. and D. Kaufmann (1999), Towards Transparency in Finance and Governance, World Bank.

Wallace, W.A., (1980) The Economic Role of the Audit in Free and Regulated Markets, Graduate School of Management, University of Rochester, NY.

Werbach K. (2016). Trust, But Verify: Why the Blockchain Needs the Law. 33 Berkeley Tech. L.J. 489 [online] Available at: http://ssrn.com/abstract=2844409 [Accessed 21.03.2019]

Werbach K. & Cornell N. (2017) "Contracts Ex Machina," Duke Law Journal 67(2).

Werbach K. (2018) The Blockchain and the New Architecture of Trust (Information Policy). The MIT Press.

White Fc. L. (1997) 'Technological Change, Financial Innovation, and Financial Regulation in the U.S.: The Challenges for Public Policy', May pp. 27.

Wilson, R. (1968) On the theory of syndicates. Econometrico, 36. 119-132.

Wong A. (2016). The Untold Story Behind Saudi Arabia's 41-Year U.S. Debt Secret. [online] Available at: https://www.bloomberg.com/news/features/2016-05-30/the-untold-story-behind-saudi-arabia-s-41-year-u-s-debt-secret [Accessed 14.05.2019].

Wirdum V. A. (2017). A Bitcoin Beginner's Guide to Surviving a Coin-Split. [online] Available at: https://Bitcoinmagazine.com/articles/beginners-guide-surviving-coin-split/ [Accessed 12.03.2019].

Zcash (2019) Zcash is a privacy-protecting, digital currency built on strong science. [online] Available at: https://z.cash [read 09.06.2019]

Zheng, Zibin, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. (2017). "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." In IEEE International Congress on Big Data (BigData Congress), 557–64. Honolulu, HI, USA: IEEE. https://doi.org/10.1109/BigDataCongress.2017.85.