



Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Distributed Ledger Technology – A Solution To Bank Failure?

Henry Joachim Kroeger

A dissertation submitted to the University of Dublin
in partial fulfilment of the requirements for the degree of
M.Sc. in Management of Information Systems.

2019

Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university. I further declare that this research has been carried out in full compliance with the ethical research requirements of the School of Computer Science and Statistics.

Signed: _____

Henry Joachim Kroeger

Date: 29. April 2019

Permission to lend and/or copy

I agree that the School of Computer Science and Statistics, Trinity College may lend or copy this dissertation upon request.

Signed: _____

Henry Joachim Kroeger

Date: 29. April 2019

Acknowledgements

My deepest thank you goes to Professor Khurshid Ahmad for his supervision and tireless support in the creation of this thesis.

To Diana Wilson, Brian O’Kane, and all other TCD lecturers: thank you for two years of great lectures.

To my beloved wife Lina: for her patience and support during the last two years of the program.

Abstract

With the advent of the global financial crisis in 2008, an unknown entity, Satoshi Nakamoto, published a whitepaper detailing the concept of a distributed ledger technology platform: Bitcoin. Over the last ten years, Nakamoto's initial idea has evolved and sparked various follow-up technologies taking advantage of peer-to-peer networking, fast internet based data exchange and advanced cryptography. Transactions and data stored in a distributed ledger are considered to be immutable and tamperproof, while also allowing verification by other members of the network. In this, the technology appears to be the ideal solution to prevent data mismanagement. This research attempts to provide a solution to bank failure caused by information mismanagement. It explores banking failure via publicly available data in the United States of America and Europe, as well as individual cases of information mismanagement at Lehman Brothers and Anglo Irish Bank. Based on an extensive literature review of distributed ledger technology, information management and associated technologies, as well as an analysis of contract law, the thesis discusses improvements to financial services data management, the auditing process and regulatory access to data utilizing Blockchain based smart contracts. Additionally, based on a case study of Bitcoin, it discusses disadvantages of distributed ledger technology, such as environmental impact via demands on energy consumption. It appears Blockchain and similar technologies will play an important role in addressing banking failure in the future, once the technology advances sufficiently.

Table of Contents

Declaration	i
Permission to lend and/or copy	ii
Acknowledgements	iii
Abstract.....	iv
List of Figures.....	1
List of Tables.....	3
List of Abbreviations	4
Chapter 1 – Introduction.....	6
1.1 Bank Failures and New Technologies	7
1.3 Distributed Ledger Technology and Blockchain	10
1.4 Research Question	12
1.5 Contribution	12
1.6 Structure of the Thesis.....	15
Chapter 2 – Banking Failure.....	16
2.1 Introduction.....	16
2.2 Pattern of Bank Failures in the United States of America	16
2.3 Pattern of Bank Failures in Europe	22
2.4 What leads to Bank Failure in real Cases?	23
2.4.1 The Case of Anglo Irish Bank.....	25
2.4.2 The Case of Lehman Brothers.....	25
2.4.3 Information Secrecy at other Banks.....	26
2.4.4 Information Mismanagement by the Big Four	26
2.5 Conclusion.....	27
Chapter 3 – Distributed Ledger Technology and (Smart) Contracts.....	29
3.1 Introduction.....	29
3.2 Contracts	29
3.3 Contract Management	32
3.4 Blockchain based Smart Contracts	33

3.4.1 Blockchain Architecture	34
3.4.2 Consensus Mechanisms	41
3.4.3 Smart contracts	47
3.5 Conclusion	50
Chapter 4 – Case Study: Bitcoin vs. Fiat Currency	52
4.1 Introduction	52
4.2 Distributed Ledger Technology – Bitcoin	52
4.2.1 The Tragedy of the Commons and Bitcoin’s Answer	52
4.2.2 Conducting Business with Bitcoin	56
4.2.3 Environmental impact of Bitcoin	58
4.2.4 Bitcoin Volatility	60
4.3 Conclusion	60
Chapter 5 – Summary	62
5.1 Lessons Learned	65
5.1.1 Distributed Ledger Technology – a Two Edged Sword	65
5.1.2 Data on Failed Banks in Europe	68
5.1.3 The Unclear Legal Situation of Distributed Ledger Technology	68
5.2 Conclusion	69
Works Cited	70
Appendices	86
Appendix A	86
Appendix B	87
Appendix C	89

List of Figures

Figure 1: Four types of information failure	7
Figure 2: Global database ranking (Statista, 2019).....	8
Figure 3: Overview of the InnoDB Cluster Architecture (MySQL Documentation Team, 2019).....	9
Figure 4: Network topography for different ledger systems (Swanson, 2015, p. 1)	10
Figure 5: Current, simplified auditing process chart.....	13
Figure 6: Simplified auditing process chart for distributed ledger.....	14
Figure 7: Failed U.S. banks 1934 to 1954	18
Figure 8: Failed U.S. banks 1955 to 1975	18
Figure 9: Failed U.S. banks 1976 to 1996	19
Figure 10: Failed U.S. banks 1997 to 2017	19
Figure 11: USD lost through banking failure from 1986 to 1996.....	20
Figure 12: USD lost through banking failure from 1997 to 2017.....	20
Figure 13: All FDIC insured institutions from 1990 to 2018.....	21
Figure 14: Approximation of failed European Banks.....	23
Figure 15: Major Irish banking institution auditors 2002 to 2010 (House of the Oireachtas, 2016, p. 71).....	24
Figure 16: OECD GDP per capita (measured in 2010 PPP USD) (Ollivaud & Turner, 2014, p. 45).....	27
Figure 17: Median Costs of Litigation by Case Type (Hannaford-Agor, 2013, p. 26).....	31
Figure 18: Example of a contract life cycle management workflow (Sommers & Conaughton, 2018).....	32
Figure 19: A sample Blockchain (Zheng, et al., 2018, p. 4).....	34
Figure 20: Example of a Block structure (Zheng, et al., 2018, p. 4)	35
Figure 21: Schematic comparison: traditional database vs. public ledger (Ølnes, et al., 2017, p. 358)	36
Figure 22: Degrees of centralization in different DLTs (Walport, 2016, p. 35).....	37
Figure 23: Example of a digitally signed transaction (Zheng, et al., 2018, p. 5)	38
Figure 24: Process of Block creation (Froystad & Holm, 2015, p. 10).....	39
Figure 25: Example of forked Blockchain branches (Zheng, et al., 2018, p. 8)	40
Figure 26: Sketch of a double-spending attack (Karame, et al., 2012, p. 909)	40
Figure 27: Trusted 3rd party interaction (Park & Park, 2017, p. 8).....	41
Figure 28: Round Robin with 6 participating nodes (Ranganathan, et al., 2001, p. 9).....	45
Figure 29: Blockchain technology subdomains (Morabito, 2017, p. 32)	47
Figure 30: Distributed Ledger Themes (Maull, et al., 2017, p. 484)	50

Figure 31: Coinranking screenshot (Coinranking, 2019a).....	54
Figure 32: Coinbase screenshot (Coinbase, 2019).....	54
Figure 33: CoinMarketCap screenshot (CoinMarketCap, 2019).....	54
Figure 34: Service provider support for cryptoasset (Rauchs, et al., 2018, p. 30).....	55
Figure 35: Transaction volumes and number of payments on multiple DLTs (Rauchs, et al., 2018, p. 37)	55
Figure 36: ATMs accepting cryptoassets - net changes globally (Coin ATM Radar, 2019b)	56
Figure 37: Bitcoin currency exchange price (USD) development 2014 to 2019 (Coinranking, 2019b).....	58
Figure 38: Bitcoin energy consumption (Digiconomist, 2019a)	59
Figure 39: Estimated energy consumption range for six major DLTs (Rauchs, et al., 2018, p. 82).....	59
Figure 40: Hype Cycle for Emerging Technologies, 2018 (Panetta, 2018).....	65
Figure 41: Primary Blockchain studies distribution per year (Konstantinidis, et al., 2018, p. 392).....	66
Figure 42: Flowchart to identify Blockchain use cases (Yaga, et al., 2018, p. 42).....	67

List of Tables

Table 1: Total amount of failed U.S. banks per 20 year period	17
Table 2: The prisoner's dilemma applied to the tragedy of the commons.....	52
Table 3: U.S. Bank failure rate 1990 to 2017	86

List of Abbreviations

ABOTA	American Board of Trial Advocates
ADR	Alternative Dispute Resolution
ATM	Automated teller machine
ATMIA	ATM Industry Association
API	Application Programming Interface
B.C.	Before Christ
CARB	Chartered Accountants Regulatory Board
CAS	Conditional Access System
CDO	Collateralized Debt Obligation
CLM	Contract Life Cycle Management
DAO	Decentralized Autonomous Organization
DBMS	Database Management System
DLT	Distributed Ledger Technology
DoS	Denial-of-Service
DRM	Digital Rights Management
ECB	European Central Bank
EFDI	European Forum of Deposit Insurers
E.g.	Exempli gratia (for example)
ETF	exchange-traded fund
FDIC	Federal Deposit Insurance Corporation
Fed	Federal Reserve Bank
FSB	Financial Stability Board
FSCS	Financial Services Compensation Scheme
GAAP	Generally Accepted Accounting Principles
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GFC	Global Financial Crisis
GNI	Gross National Income
GPL	General Public License
IFRS	International Financial Reporting Standards
IAASA	Irish Auditing and Accounting Supervisory Authority
ICAEW	The Institute of Chartered Accountants in England and Wales
IMF	International Monetary Fund
IoT	Internet of Things

LII	Legal Information Institute
NDA	Non-Disclosure Agreement
NDR	Norddeutscher Rundfunk
OECD	Organisation for Economic Co-operation and Development
PBFT	Practical Byzantine Fault Tolerance
PCI DSS	Payment Card Industry Data Security Standard
PoA	Proof of Authority
PoB	Proof of Burn
PoC	Proof of Capacity
PoET	Proof of Elapsed Time
PoS	Proof of Stake
PoW	Proof of Work
PPP	Purchasing Power Parity
PWC	PricewaterhouseCoopers
RDBMS	Relational Database Management System
RR	Round Robin
SaaS	Software as a Service
SEC	Securities and Exchange Commission
TDE	Transparent Data Encryption
TWh	Terawatt Hours
TLS	Transport Layer Security
USD	United States Dollar
VCS	Virtual Currency Schemes
WDR	Westdeutscher Rundfunk Köln

*“The Times 03/Jan/2009 Chancellor on
brink of second bailout for banks.”*

Satoshi Nakamoto, Bitcoin Genesis Block.

Chapter 1 – Introduction

Human society's lifeblood is the flow and exchange of information. Throughout the ages, humans needed to communicate with each other: first to hunt together, then settling together in slowly growing groups, to help each other and ultimately trade with each other. This concept continues to endure in order to ensure humanity's survival. Though, competing groups, beliefs, society models, as well as territorial rivalry required adaptation of how information are exchanged based on environmental factors. Information did not only need to be stored lastingly, they also needed to be exchanged across distances. Spatial separation causes communication difficulties: how can a receiver be sure the message she received was truly sent by the initiator? How can she be sure the information has not been changed or read unbeknownst by a third party along the way? Modes of transport may have changed from runners and riders to give way to electronic transfer via copper cable, but these questions relating to the security and transparency of information transactions are still encountered by humanity on a daily basis. Technological advances made geographical distances irrelevant, still human exchange of information follows the same basic cryptographic principles set out in the past, just vastly improved through the usage of computers.

Paired with the exchange of information, human society has to rely on the notion of contracts, agreements made between two or more parties, enforcing everyone's adherence to the previously acknowledged and codified terms and conditions. Starting with oral accords shifting into writs of various forms, humanity continues to develop more and more sophisticated and nuanced language for systemizing and applying contracts.

All of this requires the expansion of communication systems leading to higher levels of vulnerabilities and greater chance of failure. Modern examples of these are found in all major industries: in telecommunications, consumers find themselves unable from using their mobile phones due to connection failures caused by a network software glitch. In the medical area doctors cannot access their patient files due to a database breakdown or a ransomware attack.

In the aviation industry an IT deficiency leads to aircrafts having to stay on the ground and many flights to be cancelled; or in the banking industry where clients find themselves unable to take possession of their accounts and funds, disrupting the life of many as necessary goods could not be acquired without access to the system.

These points illustrate the fundamental need to maintain data integrity at all times, for this thesis though, the focus will be on banking failures and a potential new technology solution through distributed ledger technology and smart contracts to prevent such failures in the future.

1.1 Bank Failures and New Technologies

In order to examine banking failure, a definition of what it means for a bank to fail is needed: they occur when regulatory bodies force a financial institution to either merge with another (banking) organization or to close down operations (Cebula, et al., 2011).

From the perspective of information management, banks can fail for four different reasons (Figure 1).

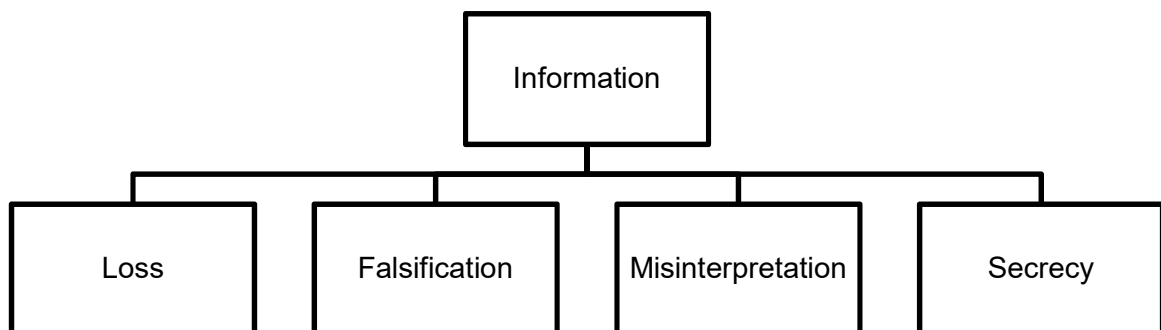


Figure 1: Four types of information failure

- Information systems can **lose** data (temporarily or permanently) through failures or human neglect in processing, storage or transmission. Temporary data loss could result from a network outage resulting in being unable to access for example a central database, while permanent data loss would occur if the storage units for this central database became corrupted. Additional risk is posed through improper backup procedures and failing in setting up a remote disaster recovery site.
- The information stored in a system can be **tampered** with intentionally by a malicious attacker or accidentally by regular users through carelessness (Schulze, 2018).

- Additionally, data can be **misinterpreted** by system users, leading for example to incorrect background checks (Elejalde-Ruiz, 2015), higher interest rates or difficulties in obtaining a credit or a mortgage (Oliver, 2016).
- Finally, it is also possible to **keep information a secret**, for example the nature and composition of collateralized debt obligation [CDO] products in advance of the 2007 subprime mortgage crisis in the United States of America (Lewis, 2010). This is the case, because clients cannot access the same information the financial institution acquires and is not always aware of what the organization does with the provided funds.

For a discussion of a current technology example, the open source technology relational database management system [RDBMS] MySQL will be analysed in the following on how it addresses the four information management challenges. Since it is currently the second most popular database globally (DB-Engines, 2019) (Figure 2), it is widely employed for data management purposes.

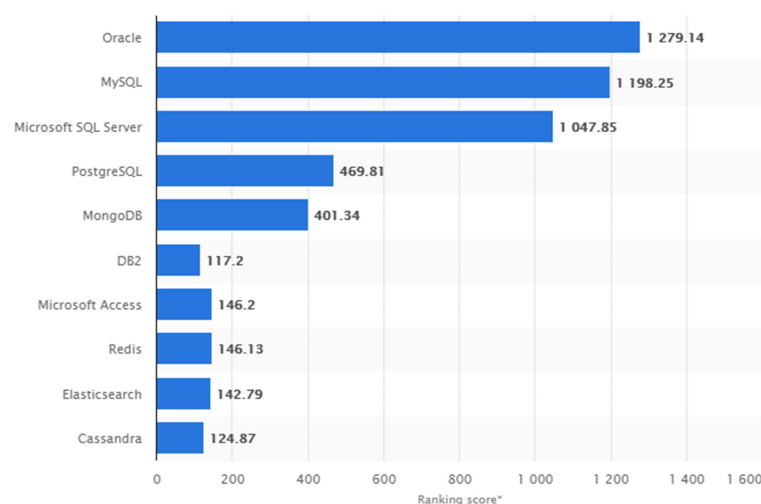


Figure 2: Global database ranking (Statista, 2019)

MySQL addresses the data management challenges secrecy, loss and immutability in the successive way (MySQL Documentation Team, 2019):

- For **security purposes** and in compliance with international and local data regulation requirements¹, MySQL features transparent data encryption [TDE]: a feature set allowing data at rest encryption and employing digital signatures, symmetric and asymmetric encryption mechanisms, as well as data authenticity validation (ibid.).

¹ For example: The Payment Card Industry Data Security Standard [PCI DSS]; the EU General Data Protection Regulation [GDPR]; the UK Data Protection Act 2018; or the Sarbanes Oxley Act of 2002.

- The risk of **information loss** on the database level is mitigated through the InnoDB Cluster, a high availability solution for the DBMS (Figure 3). Utilizing a minimum of three MySQL server nodes in order to avoid what is known as split-brain syndrome² scenarios (Schwartz, et al., 2008), the InnoDB Cluster operates the MySQL Group Replication software to ensure automatic failover in case of a breakdown of the primary database instance. In case of a breakdown, one of the secondary MySQL instances will automatically be promoted to be the new primary instance and the MySQL Server will reroute the application traffic accordingly.

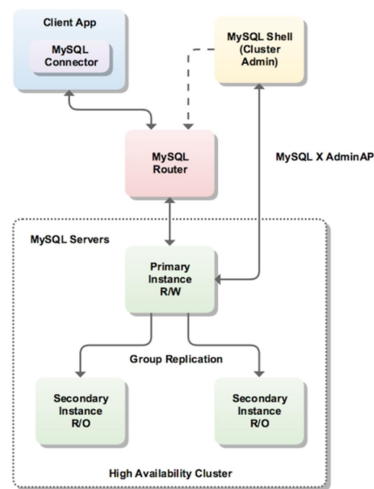


Figure 3: Overview of the InnoDB Cluster Architecture (MySQL Documentation Team, 2019)

- **Data Tampering**, in the case of MySQL, is prevented through an SQL whitelist, limiting SQL statement executions to pre-approved code patterns (MySQL Documentation Team, 2019). It is also documented, that an automated auditing tool allows the database administrator to set-up policies for logging and monitoring query and connection activities on any given MySQL server instance.

MySQL serves as an illustration only, other database management systems such as Microsoft's SQL Server, PostgreSQL or Oracle database, employ similar systems to make use of peer to peer networks and encryption to ensure data integrity.

Despite these software instruments as well as redundant networks and servers, banks continue to fail in their information management tasks. This is because of the information asymmetry between patron and bank. In fact, the presumption of non-immutable contracts between both parties is a risky assumption and not guaranteed. The client in such cases finds herself disadvantaged.

² In case of a split-brain syndrome, two database server instances are trying to promote themselves to primary node at the same time.

In pursuance of proposing a technological solution to this information management challenge, this thesis explores self-enforcing Blockchain based smart contracts as new information management system to avoid banking failures.

1.3 Distributed Ledger Technology and Blockchain

A centralized ledger like a database requires a controlling entity for synchronization and system maintenance since only the entity keeps a copy of the ledger. In a distributed ledger system on the other hand, all participants of the network hold a full copy of the transaction ledger (Burkhardt, et al., 2018). The step in between the centralized and distributed systems can be considered as a decentralized ledger in which only few members of the network hold a copy of the full ledger. All three network topographies are illustrated in Figure 4.

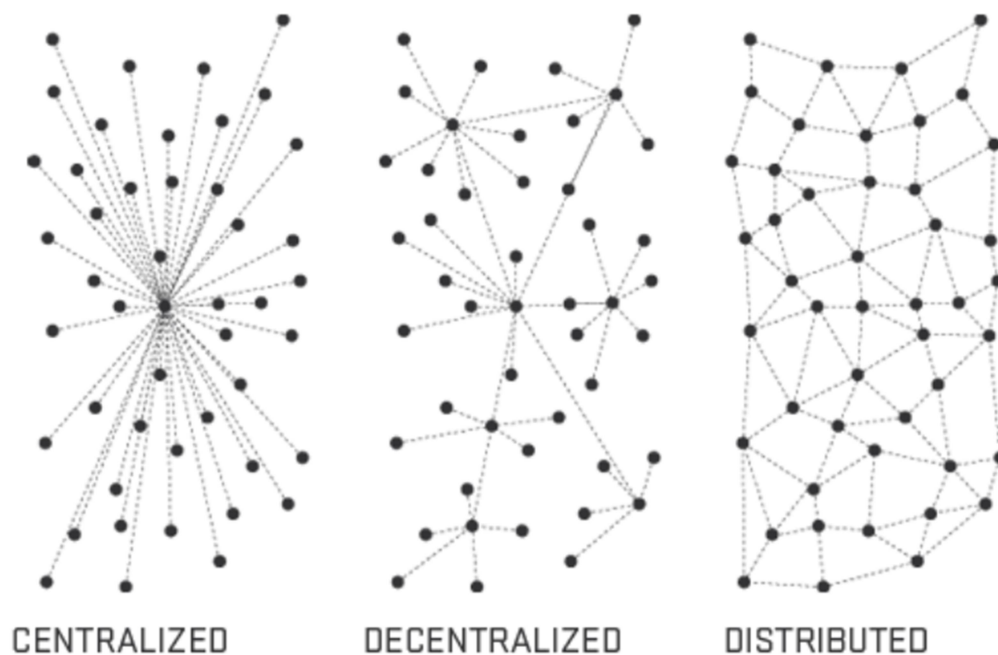


Figure 4: Network topography for different ledger systems (Swanson, 2015, p. 1)

Before delving further into the nature of the distributed ledger technology it is necessary to explore the origins of ledgers and their importance to human information collection.

The Merriam-Webster dictionary defines a ledger as “*a book containing accounts to which debits and credits are posted from books of original entry*” (Merriam-Webster, 2018). It is one of two books operated in the process of bookkeeping; the other one being the journal in which daily transactions are being collected (The Editors of Encyclopaedia Britannica,

2018). These original entries in the journal are then transferred to the ledger in which they are summarized by account. Early examples of similar economic record keeping can be traced back to the Hellenistic period and the Ptolemaic dynasty from 305 to 30 B.C, as well as the Roman Empire: In order to rule Egypt efficiently, the royal Ptolemaic family built a vast administration to control economic activity and collect taxes as well as keep records about land, labour and policies (Engen, 2018), while the Roman banking system is considered to be “*nearly as high a development as our own*” (Hoggson, 1926, p. 40).

Bookkeeping plays an important role throughout human history for governance and administration, but particularly the development of what Goethe called “*eine der schönsten Erfindungen des menschlichen Geistes*” [“one of the most beautiful inventions of human ingenuity”] (von Goethe, 1798), double-entry bookkeeping is considered a decisive event in the economic history Europe’s (Spengler, 1928).

This notion is supported by Max Weber and others (Carruthers & Nelson Espeland, 1991). Weber writes for example: “*The most general presupposition for the existence of this present-day capitalism is that of rational capital accounting as the norm for all large industrial undertakings [...]*” (Weber, 1981, p. 276). Nonetheless it is an assumption not without controversy, as some have argued that evidence for this hypothesis is scarce and does not fully correlate with the emergence of early forms of capitalism (Bryer, 1993) (Yamey, 1949). Similar ambiguity also governs the origin of the double-entry technique: while researchers agree, that this approach first emerged in 14th century Italy³ (Riccaboni, et al., 2006) (Bisaschi, 2003), they disagree on the exact location. Arguments have been made for Venice (Gleeson-White, 2011), Florence (Sangster, 2016) and Siena (Martinelli, 1974), but no conclusive result has been agreed upon.

Over time the Italian principles developed into the modern accounting frameworks known as International Financial Reporting Standards [IFRS] and the US based Generally Accepted Accounting Principles [GAAP] that form the basis for international taxation (Vanoli, 2005).

With the advance of modern computer technology, starting with the Universal Turing Machine (Turing, 1937) and the von Neumann architecture (von Neumann, 1993), these leather bound, paper based ledgers moved into the electronic world of bits and bytes and were stored in centralized database software solutions. This equated physical written ledgers with electronically stored databases with handwriting being replaced with read/write commands. While these, over time and with respect to system resilience, became decentralized databases with redundancies between them, they are still

³ This is why the double-entry bookkeeping is often called the “Italian Method”.

controlled by an individual organization. Distributed ledger technology is offering the potential to change this, an open up these information storages to the general public.

1.4 Research Question

This thesis is examining two research questions:

1. Has information mismanagement contributed to banking failure during the global financial crisis from 2008 to 2012?
2. Can distributed ledger technology address this information handling negligence and provide a solution to minimize the risk of future large scale bank failures?

1.5 Contribution

While answering the two research questions, focusing on information systems, this thesis provides an understanding of information loss and consequences in a financial services context. Specifically banking failure in the United States and in Europe is being analysed based on publically available data through the LexisNexis News and Business portal and the U.S. American Federal Deposit Insurance Corporation database⁴. The indexes of the CIA World Fact Book, the International Monetary Fund and the World Bank are used for global population and energy consumption statistics. Additionally, this thesis provides an understanding of distributed ledger, Blockchain and smart contract technology.

It provides a new potential solution to literature on banking failure and the global financial crisis from an information systems management perspective.

This solution is a move from the current auditing and information management process (Figure 5) for financial services, to a new process (Figure 6) utilizing public, permissionless distributed ledger technology providing full access to all ledger transactions to auditors, regulators and the general audience alike.

⁴ All used data and created graphs can be accessed and downloaded in this excel spreadsheet: https://www.dropbox.com/s/516srgl5148dxuh/hjk_msc%20mis_thesis_distributed%20ledger%20technology%20-%20a%20solution%20to%20bank%20failure_datasheet.xlsx?dl=0

- **Figure 5:** Currently, statutory banking audits are carried out on a regular basis through an external auditor, for example the company KPMG. This auditor is accessing the institutions transaction ledgers and bookkeeping records in order to compile an auditing report. This report in turn, is presented to regulators so they can assess legal and regulatory compliance of the audited bank, as well as the general populace. Neither the general audience, nor the regulator is given full access to all ledgers and records unless legally required.

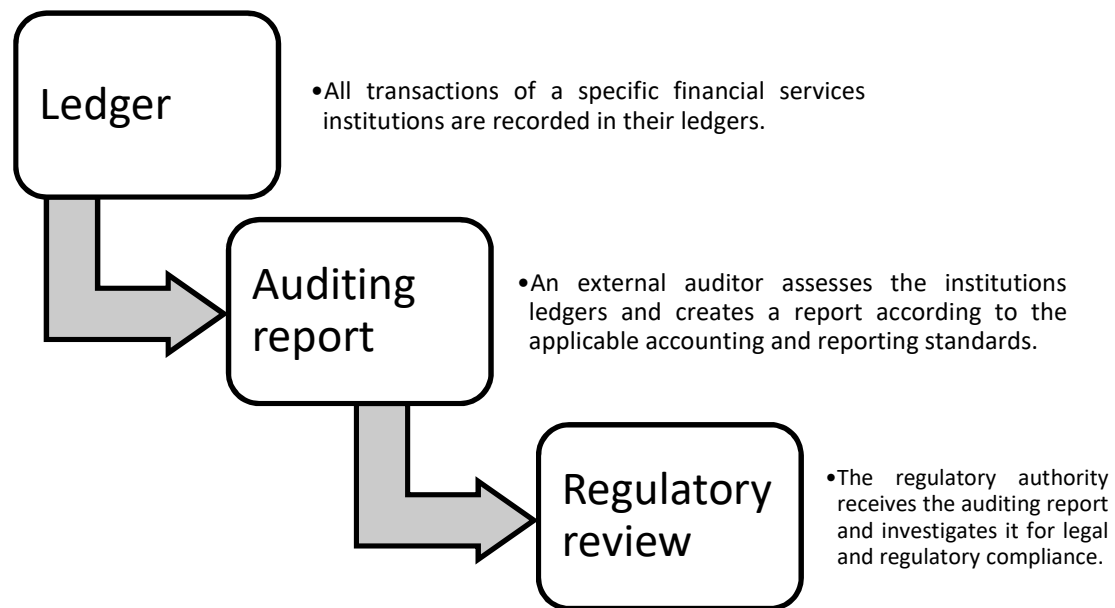


Figure 5: Current, simplified auditing process chart

- **Figure 6:** Instead of utilizing a centralized ledger in form of an electronic database, this thesis proposes for financial services institutions to work with a publicly accessible, immutable, distributed ledger with smart contract capability. This allows auditors, regulators and the general audience to access all transactions at any given time, and verify all information themselves, without relying on potentially incorrect auditing reports.

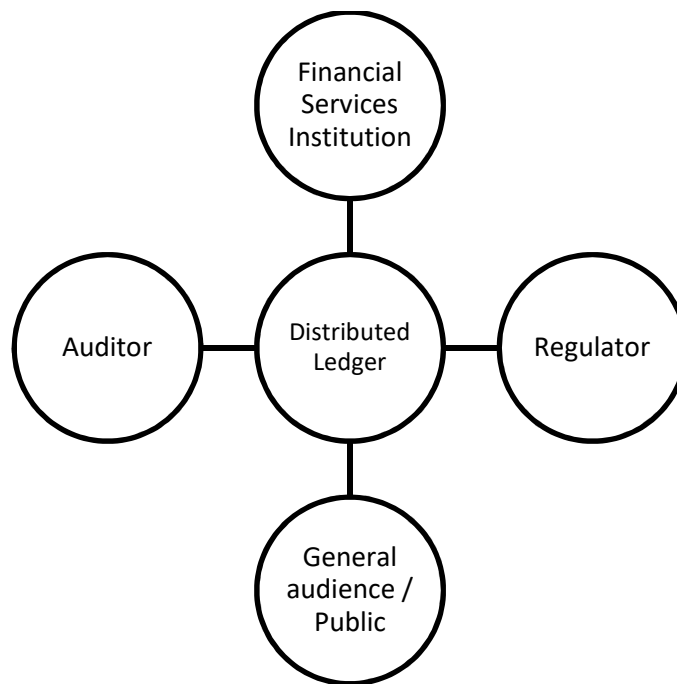


Figure 6: Simplified auditing process chart for distributed ledger

1.6 Structure of the Thesis

The thesis is divided in five parts:

Chapter 1 provides an introduction to the topic of information management and distributed ledger technology, as well as giving a brief history of the development of ledgers. It also contains the two research questions framing the thesis and indicates the new contribution to the existing body of literature.

Chapter 2 analyses and quantifies patterns of banking failure in the United States and Europe over the last 100 years, as well as determines some exemplary cases in which information mismanagement contributed towards said failure.

Chapter 3 discusses the basic legal parameters for contracts as well as modern contract management before investigating Blockchain architecture, consensus mechanisms and smart contracts.

Chapter 4 provides a case study on Bitcoin as an example of distributed ledger technology, deliberating the tragedy of the commons in networking technology, Bitcoin usage, the possibility of business transactions, the environmental impact and the volatility of the associated cryptocurrency.

Chapter 5 concludes the thesis, provides a summary of the findings as well as lessons learned and briefly gives an outlook to the future.

Chapter 2 – Banking Failure

2.1 Introduction

Financial institutions fulfil a specific role in the (global) economy as a “*relationship-based lender with hard-to-replace informational advantages vis-à-vis small- and medium-sized firms*” (Bhattacharya & Nyborg, 2013, p. 29) as well as consumers. These advantages result from an information asymmetry about the condition of the institutions assets and investments: whether these are illiquid, risky or troubled is in most cases unknown to the bank’s clients. Additionally, debt overhang⁵ can occur because of incomplete financial contracts (Bulow & Shoven, 1978) (Philippon & Schnabl, 2013), as well as extensive re-negotiation cost (Hennessy, 2004) and thus lead to bankruptcy or bailout risk. A possible technical solution to remedy information mismanagement in the financial sector will be explored in chapter 3. In the following the financial depth of the problem will be explored based on failed banks in the United States of America as well as in Europe. Additionally cases of information mismanagement and misconduct at financial services firms, as well as auditors will be presented and discussed.

2.2 Pattern of Bank Failures in the United States of America

As of 1933, the Federal Deposit Insurance Corporation [FDIC] is an independent agency of the U.S.-American federal government responsible for the promotion and the preservation of citizens’ confidence in the U.S. financial system (FDIC, 2017). It insures bank deposits for at least 250,000.00 USD and is funded through insurance premiums collected from banks and thrift institutions, as well as through investments in U.S. Treasury securities. Following a number of recessions after the end of World War I, at least partly caused through a “*chaotic banking structure*” (Alper, 1933, p. 194), the Senate and the House of Representatives of the United States of America implemented the Banking Act of 1933 (Congress United States of America, 1933) leading to the creation of the FDIC (Preston, 1933). Besides deposit insurance, the organization is also responsible for auditing financial institutions on consumer protection law compliance as well as answer immediately in case of a bank failure. As part of its federal political mandate the FDIC collects, compiles and provides data on all failures of its insured institutions⁶ since its inception in 1933.

⁵ Debt overhang is a debt burden large enough to prevent any entity to acquire new debt to finance future projects.

⁶ All data can be accessed and downloaded here: <https://banks.data.fdic.gov/explore/failures>.

A review of the dataset from the FDIC course reveals this:

Splitting the data⁷ into 20 year terms and plotting the total number of failed banks (y-axis) across four different periods (x-axis) – 1934 to 1954, 1955 to 1975, 1976 to 1996, and 1997 to 2017 – results in the graphs displayed in Figure 7 to Figure 10.

Table 1 on the other hand, presents the overall number of failed banks in all four terms.

Period	Name	Total amount of failed banks
1934 – 1954	A	424
1955 – 1975	B	98
1976 – 1996	C	2989
1997 – 2017	D	585

Table 1: Total amount of failed U.S. banks per 20 year period

⁷ All used data and created graphs can be accessed and downloaded in this excel spreadsheet:
https://www.dropbox.com/s/516srgl5148dxuh/hjk_msc%20mis_thesis_distributed%20ledger%20technology%20-%20a%20solution%20to%20bank%20failure_datasheet.xlsx?dl=0

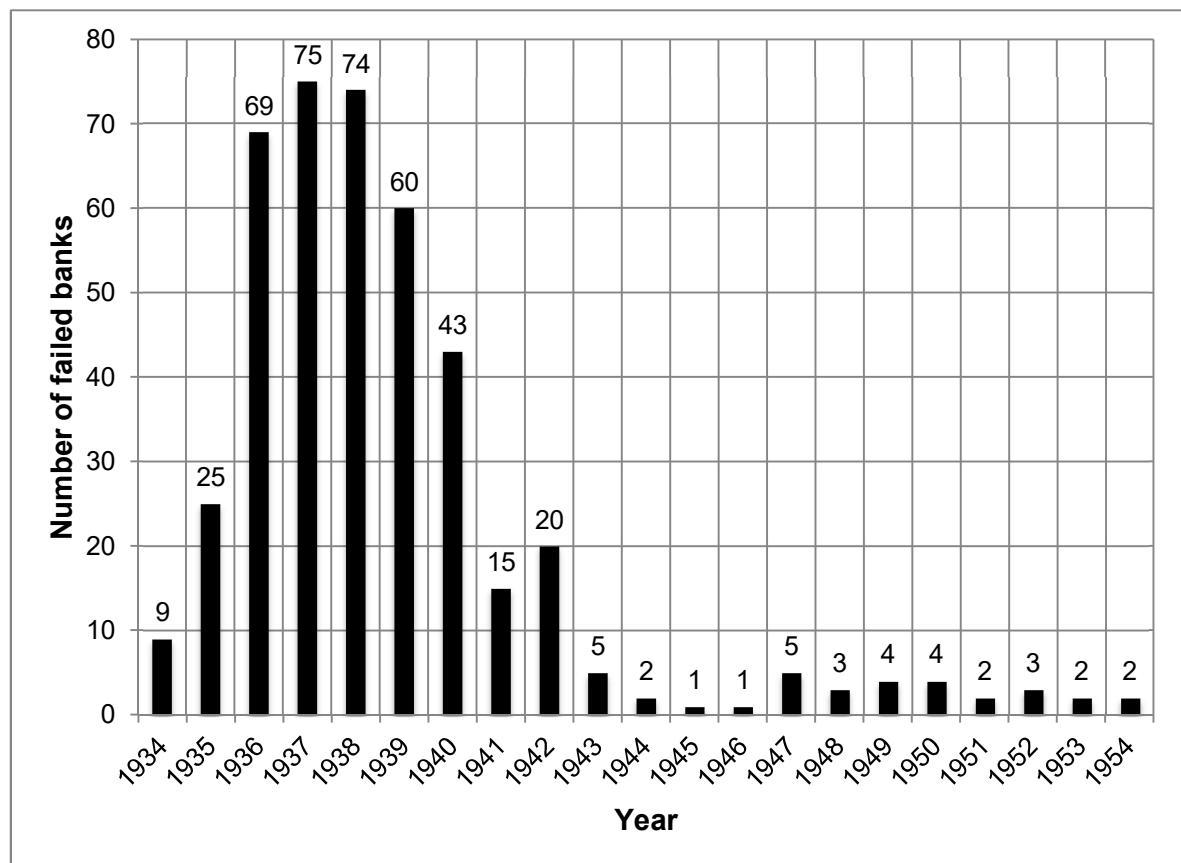


Figure 7: Failed U.S. banks 1934 to 1954

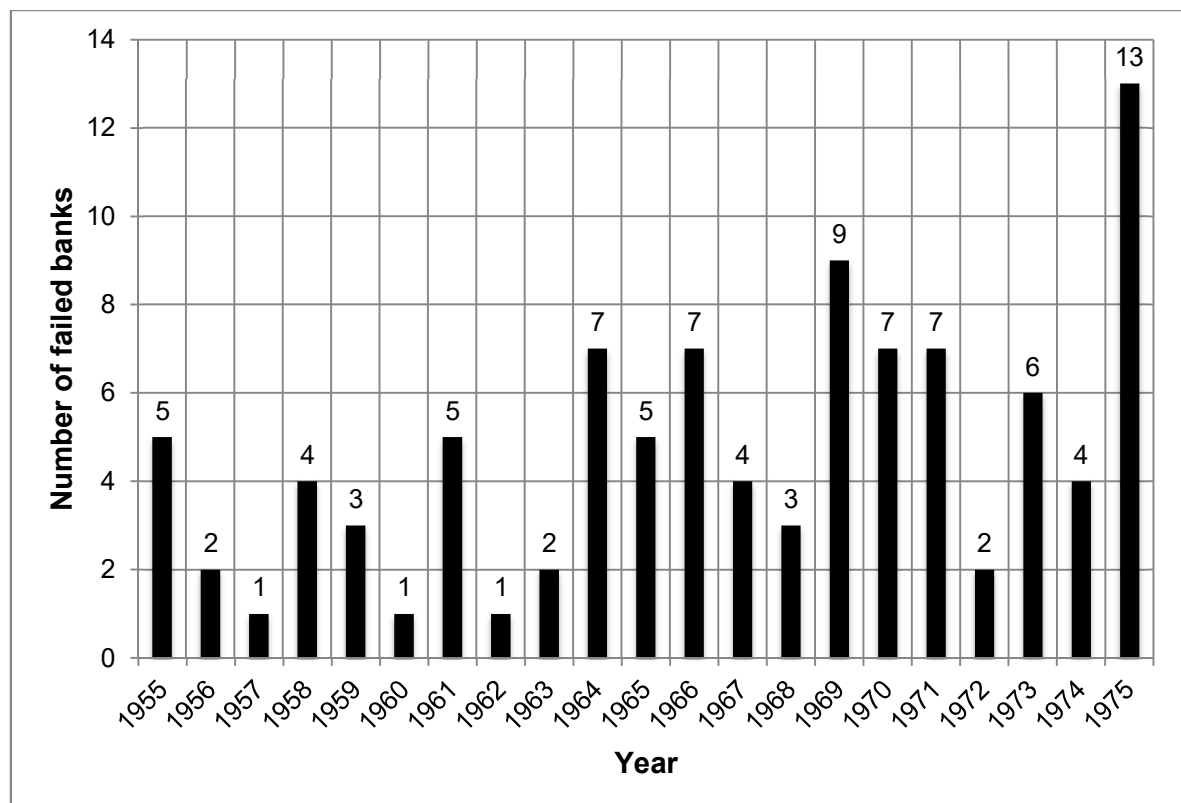


Figure 8: Failed U.S. banks 1955 to 1975

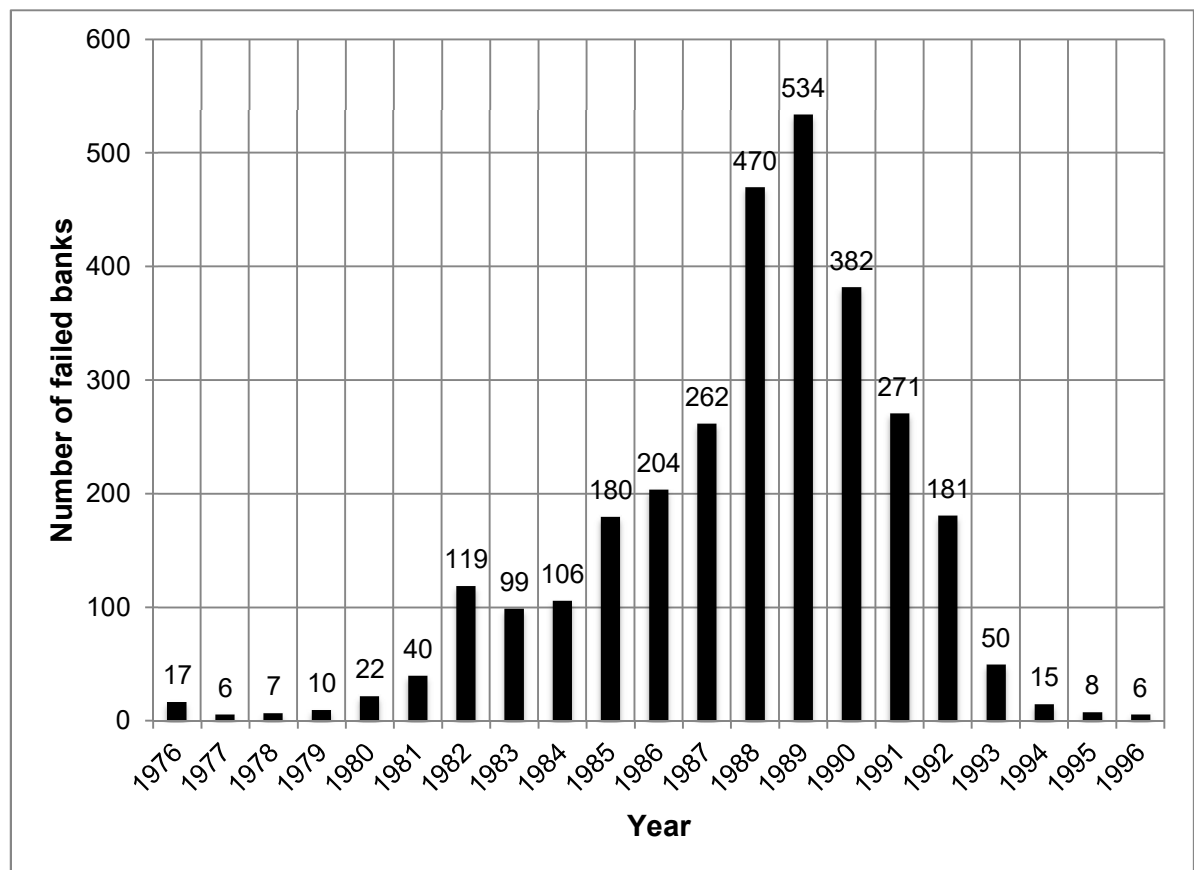


Figure 9: Failed U.S. banks 1976 to 1996

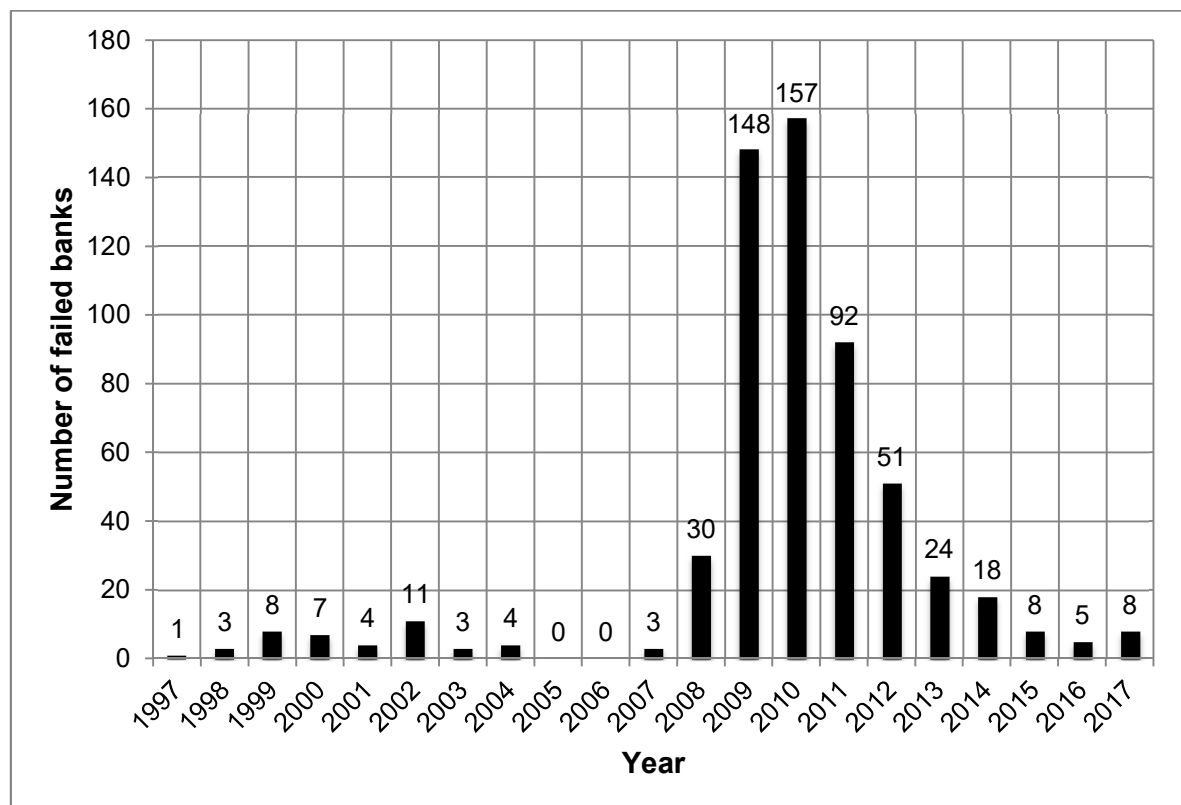


Figure 10: Failed U.S. banks 1997 to 2017

The same dataset also contains information on the estimated loss of the insured, failed institutions in the two periods 1986 to 1996 (Figure 11) and 1997 to 2017 (Figure 12).

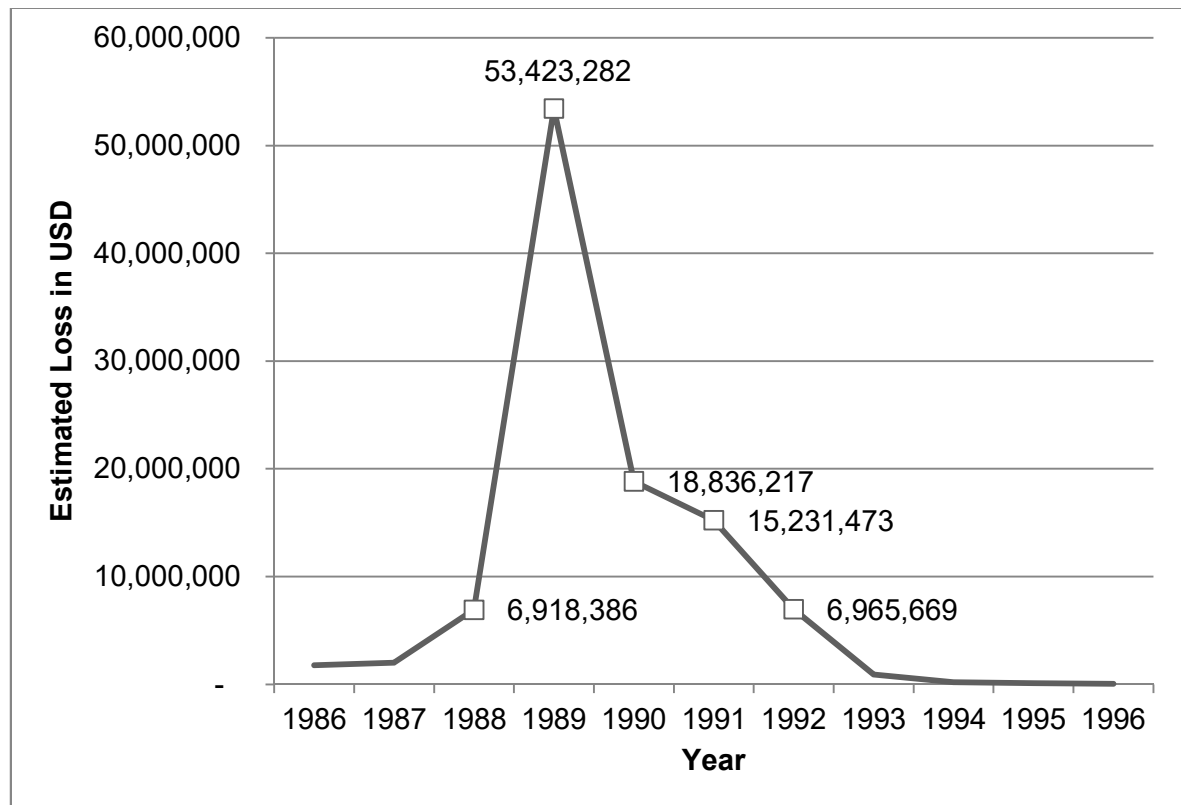


Figure 11: USD lost through banking failure from 1986 to 1996

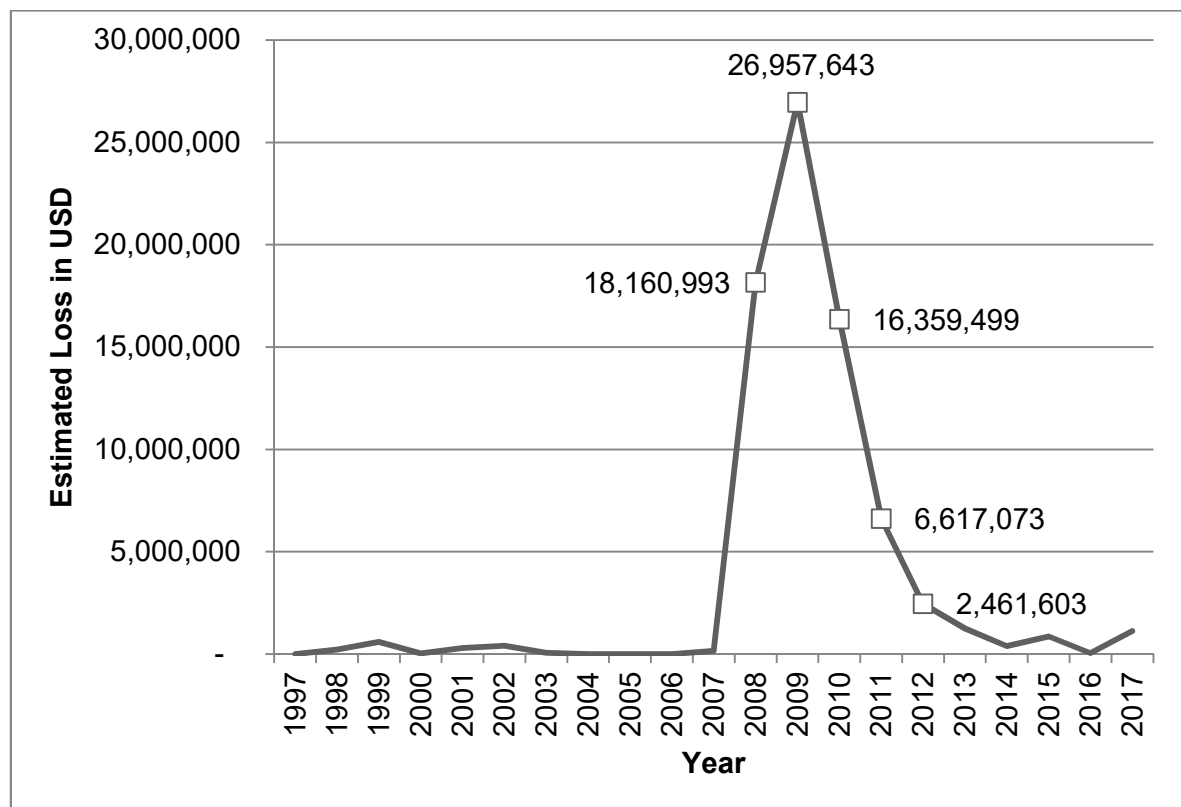


Figure 12: USD lost through banking failure from 1997 to 2017

Additionally, the FDIC provides a dataset on all financial institutions insured with them since 1990⁸. Figure 13 maps the number of FDIC insured banks (y-axis) over a period of 28 years from 1990 to 2018 (x-axis):

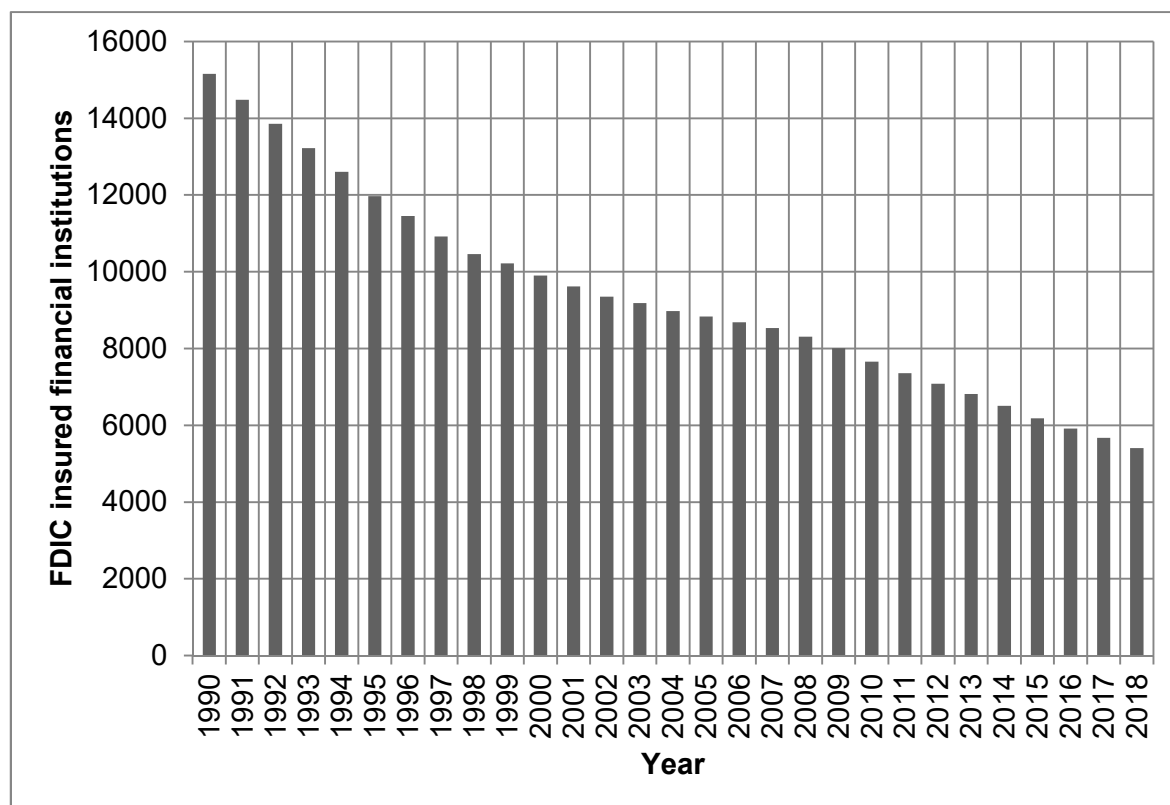


Figure 13: All FDIC insured institutions from 1990 to 2018

Upon inspection it becomes visible, that the amount of banks in the United States has been declining year over year. This downturn is confirmed by Berger, et al. (1995) and Jones & Critchfield (2005). They are attributing it to changes in the regulatory controls of the U.S. government and advances in technology removing restrictions in geographical limitations for office branches.

Contrasting the data forming the basis for Figure 13 with the amount of failed FDIC insured banks from Figure 9 to Figure 10 for the period 1990 to 2017⁹ leads to Table 3 in Appendix A and allows calculation of the mean of the banking failures from 1997 to 2017: 0.38%. In their 2011 study, Cebula, et al. found the U.S. banking failure rate for the period 1970 to 2009 to have a Mean of 0.339 with a Standard Deviation of 0.49 (Cebula, et al., 2011, p. 43).

⁸ The original FDIC dataset “December 2018 Statistics – FDIC Historical Trends” can be accessed here: <https://www.fdic.gov/bank/statistical/stats/>.

⁹ The FDIC does not yet provide data on how many banks failed in 2018.

The United States of America experienced three periods of large amounts of bank failures: the first one from 1936 to 1940 (Figure 7) right after the introduction of the 1933 Glass-Steagall Act introducing restrictions and regulations to banking activities, “*effectively separating commercial and investment banking [...]*” (Shughart, 1988, p. 595) where some financial institutions were not able to survive the legal changes. The second one from 1982 to 1993 (Figure 9), named savings and loan crisis, as well as “*the greatest collapse of U.S. financial institutions since the 1930s*” (Curry & Shibut, 2000, p. 26), was the result of volatile and high interest rates, deregulation and a number of other factors (ibid.). Estimated costs for taxpayers are USD 124 billion (ibid.). The third and most recent period of bank failures from 2008 to 2012 (Figure 10) was the result of the subprime mortgage crisis (Demyanyk & Van Hemert, 2009). The FDIC dataset indicates a loss of about 70.5 million USD exclusively due to bankruptcy of some of their members. The overall loss of the crisis and U.S. government reactions to it, is much more difficult to assess and no clear numbers are given (GAO, 2013) (Webel & Labonte, 2018).

2.3 Pattern of Bank Failures in Europe

Unlike the centralized federal organization of the FDIC in the United States of America, in Europe, a similarly tasked central organization does not exist for all European countries. The closest European institution to the FDIC is the European Forum of Deposit Insurers [EFDI], but instead is a non-profit international association of 72 national deposit insurance institutions of 47 countries located in Europe¹⁰. It does not have a political mandate, an instead serves as a platform for the communication exchange of the various national establishments on financial deposit protection. While the EFDI conducts a variety of research projects, e.g. on European banking stress tests, it does not publish statistics on failed financial institutions as the FDIC does. The same is true for the national deposit insurers: if statistics are being published, they contain information about their deposits and the amount of insurance liabilities, and in a few instances name some nationally failed firms (for example in case of the British Financial Services Compensation Scheme [FSCS]). Other associations or organisations, such as the International Association of Deposit Insurers [IADI] or the Financial Stability Board [FSB], also do not publish a list of failed banks in Europe. Taking into consideration the limited available statistics and public data, as well as using LexisNexis’ Nexis database, Google and some national deposit protection agency’s publications in English allows the creation of the non-exhaustive list of failed European financial institutions from 2007 to 2019 in Appendix B. Visualizing this list via plotting the amount of failed banks (y-axis) across the time period results in Figure 14.

¹⁰ <https://www.efdi.eu/>

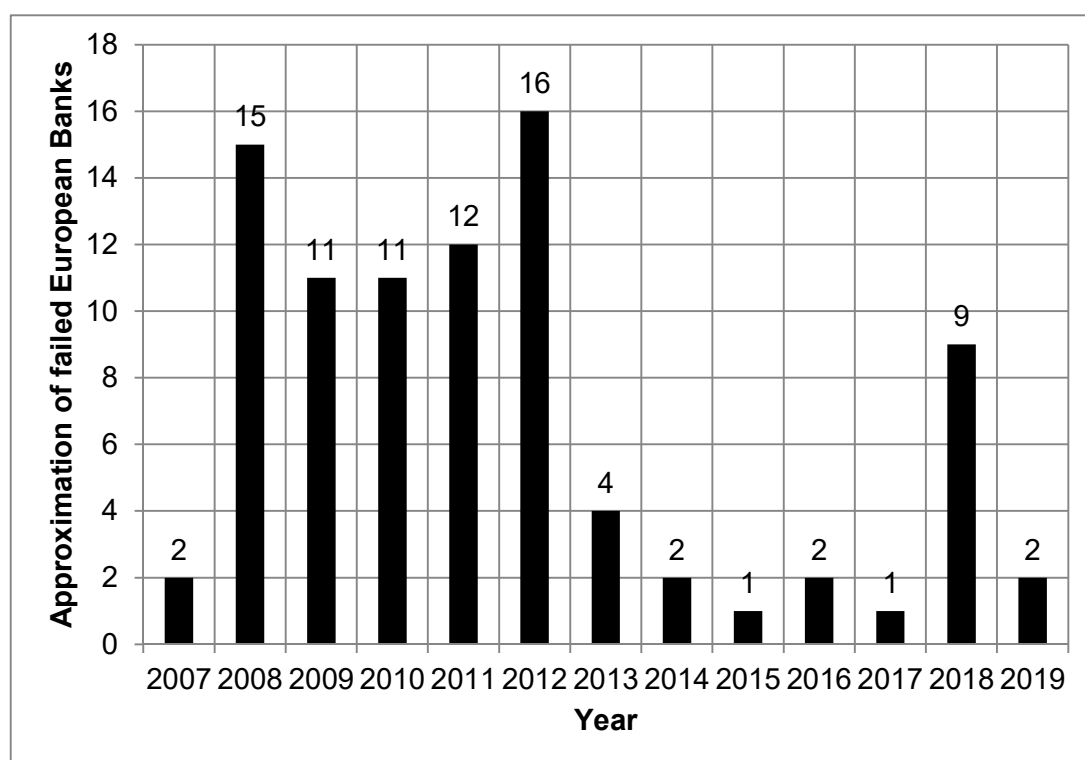


Figure 14: Approximation of failed European Banks

Despite the European public data being much more limited than the U.S. statistics provided through the FDIC a comparison between Figure 14 and Figure 10 reveals a similar pattern of high amounts of bank failures between 2008 and 2012 in context of the subprime mortgage crisis in the United States of America and the resulting global financial crisis.

2.4 What leads to Bank Failure in real Cases?

Commercial and investment banks find themselves subject to statutory internal (via legally required internal auditing structures) and external auditing through regulatory bodies, for example the Central Bank of Ireland or the Irish Auditing and Accounting Supervisory Authority [IAASA]. While the external audit only takes place once or twice a year, internal auditing functions fulfill a continuous role of preventing the firms exposure to fraud or risks in compliance with all local legal and regulatory obligations. Financial institutions often choose to work with an external, independent auditing firm to compile the (bi-) annual reports submitted to the regulatory authorities. In the banking industry, often times one of the “big four”, Deloitte, EY (formerly Ernst & Young), KPMG and PricewaterhouseCoopers [PWC], professional service providers is employed for the auditing report creation (Figure 15).

Bank	2002	2003	2004	2005	2006	2007	2008	2009	2010
AIB	KPMG	KPMG	KPMG	KPMG	KPMG	KPMG	KPMG	KPMG	KPMG
EBS	EY	EY	EY	EY	EY	EY	EY	KPMG	KPMG
BOI	PWC	PWC	PWC	PWC	PWC	PWC	PWC	PWC	PWC
Anglo	EY	EY	EY	EY	EY	EY	EY	DT	DT
PTSB	KPMG	KPMG	KPMG	KPMG	KPMG	KPMG	KPMG	KPMG	KPMG
INBS	KPMG	KPMG	KPMG	KPMG	KPMG	KPMG	KPMG	KPMG	N/A

Figure 15: Major Irish banking institution auditors 2002 to 2010 (House of the Oireachtas, 2016, p. 71)

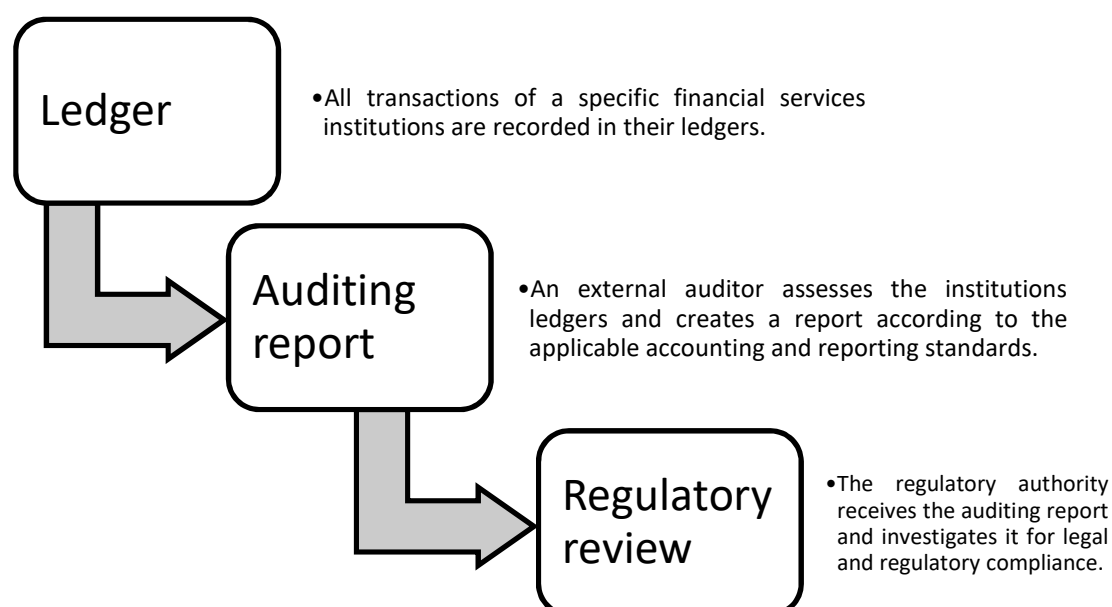


Figure 5: Current, simplified auditing process chart

Figure 5 visualizes the simplified auditing work-flow that is being followed during the statutory banking audit. Besides the regulatory authority, the public is also able to assess the report as part of the annual report of any given financial services provider. This does not grant the public access to the internal ledger of the bank though. The provided information cannot be verified and trust has to be given to the role of internal and external auditors, particularly the in the banking sector in Ireland prominently ranking big four.

This reporting process has been criticised for providing insufficient information and early warning indications of bank failures despite a plethora of information provided publicly under the Basel II accord (Prescott, 2004) and other regulatory frameworks (The Institute of Chartered Accountants in England and Wales (ICAEW), 2010). Partly, this can be attributed to one of the four types of information failure (Figure 1), the misinterpretation of information due large amount of available data. Upon the revision of data about Irish banking failures in the aftermath of the global financial crisis 2008 to 2012 though, it becomes clear that the other three types of information mismanagement (falsification, loss and secrecy) played a much larger role.

2.4.1 The Case of Anglo Irish Bank

The former chief executive officer of the former Anglo Irish Bank (now part of the Irish Bank Resolution Corporation (IBRC - Irish Bank Resolution Corporation, 2018)) David Kenneth Drumm was convicted of “*conspiracy to defraud and false accounting*” (Carswell, 2018a) resulting in artificially enlarging Anglo Irish Bank’s accounts by € 7.2 billion (Carswell, 2018b). This is an example of internal information falsification and secrecy leading to the failure of Anglo Irish Bank at the end of 2008 and the following nationalisation through the Republic of Ireland in the beginning of 2009 (O’Sullivan & Kinsella, 2011).

2.4.2 The Case of Lehman Brothers

Similar information secrecy can be found in the case of the failure of the former fourth largest investment bank globally, Lehman Brothers resulting in their filing for bankruptcy in 2008 (Jeffers, 2011): employing “*off-balance sheet devices, known within Lehman as “Repo 105” and “Repo 108” transactions*” (Valukas, 2010, p. 732) the firm was able “*to temporarily remove securities inventory from its balance sheet*” (ibid. p. 732). While such repos (sale and repurchase agreements) are commonly employed in the investment banking sector, the specific details of these transactions were “*sufficiently unusual to warrant informing Lehman’s audit committee*” (Caplan, et al., 2012, p. 447). Instead they were hidden even from “*careful review of Lehman’s 10-K and 10-Q filings*” (Valukas, 2010, p. 734). Additionally, the Repo 105 activity would increase “*substantially around quarterly reporting dates to the Securities and Exchange Commission (SEC), seemingly as a “window dressing” to reduce leverage ratios*” (Hines, et al., 2011, p. 42).

The available evidence indicates that these unusual transactions may have considerably contributed to the Lehman Brothers bankruptcy and the following global financial crisis (Jeffers, 2011).

2.4.3 Information Secrecy at other Banks

Lehman Brothers wasn't the only financial services company making use of an end-of-quarter window dressing practice as an analysis of the Wall Street Journal suggests: it appears that this activity *"has accelerated since 2008"* and that *"three big banks – Bank of America Corp, Deutsche Bank AG and Citigroup Inc. – are among the most active at temporarily shedding debt just before reporting their finances to the public"* (Rapoport & McGinty, 2010). Hiding financial risk from current and potential investors, as well as the public is not a new practice; Ketz (2003) for example identifies four different methods how to hide debt through means of accounting: the equity method, lease accounting, pension accounting and special-purpose entities. While some of those methods have been addressed through new legislation and closing of accounting standards loopholes, the problem persists.

2.4.4 Information Mismanagement by the Big Four

A recent documentation, based on research of the German newspaper Süddeutsche Zeitung (South German Newspaper) as well as the two broadcasting houses Westdeutscher Rundfunk Köln [WDR] (West German Broadcasting Cologne) and Norddeutscher Rundfunk [NDR] (Northern German Broadcasting), titled *"Die Berater der Reichen und Mächtigen - Die Macht der Big Four"* (Consultants to the rich and the powerful – the power of the big four) (2019). In their work, the authors identify the dual nature of the four firms Deloitte, EY, KPMG and PWC as auditors as well as consultants as problematic. Not only are they acting as independent auditors supervising client's regulatory compliance, they also consultant on various instances the same clients on their behaviour to be compliant, as well as work as experts with national governance on the creation of new laws and regulations. It is argued that this puts them in a unique position to assist their clients in hiding information.

The argument of misconduct at the four auditing firms is supported by an investigation launched by the special investigator John Purcell of the Irish Chartered Accountants Regulatory Board [CARB] in context with the Anglo Irish Bank bankruptcy against Anglo's auditor of time, Ernst and Young (Daly, 2011). The investigation resumed in 2018 after the prosecution of David Drumm and other Anglo personnel was concluded and the results, which could require a public, professional disciplinary hearing of EY, are still outstanding.

2.5 Conclusion

Banking failure has been a regular occurrence in Europe and the United States during the last 100 years of human history. The most recent major incident was the global financial crisis [GFC] from 2008 to 2012 leading to the collapse of many larger and smaller banking and investment firms. In a globally, interconnected world, the failure of initially few banks, led to a chain reaction causing economic loss for the years to follow. Figure 16 details the opportunity loss on OECD GDP per capita compared to pre-crisis trends.

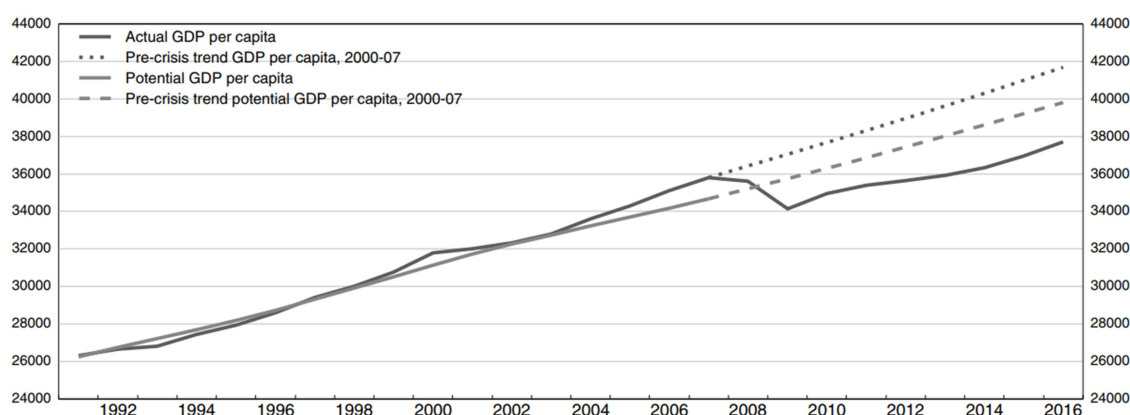


Figure 16: OECD GDP per capita (measured in 2010 PPP USD) (Ollivaud & Turner, 2014, p. 45)

While the major cause for the GFC is considered to be a real-estate bubble caused by subprime mortgage lending and a boom of credits in the United States of America (Shiller, 2008), as well as “*rapid asset price appreciation*” (Claessens & Kodres, 2014, p. 6) leading to large increases in house prices. This thesis identifies information mismanagement at financial services institutions as additional contributor to the large amount of bank failures materializing during the crisis. In a few well-documented cases it was proven that some bank executives committed fraud and that information hiding from regulators and public records was a common practice engaged by some financial institutes and auditing firms. The dual nature of some larger auditing firms, the so called big four, incorporating both auditing as well as consultative functions is questioned.

In order to provide a potential technical solution to the identified information malpractice, the following chapter three is going to explore distributed ledger technology and smart contracts as a viable alternative to current information management standards.

Chapter 3 – Distributed Ledger Technology and (Smart) Contracts

3.1 Introduction

This chapter discusses distributed ledger technology and smart contracts in the interest of examining its information handling potential to prevent banking failure. For this purpose, it begins with an inquiry into contracts and current contract management software solutions, before continuing on to Blockchain based smart contracts as one for of distributed ledger technology. Furthermore Blockchain architecture, consensus mechanisms, smart contracts and decentralized autonomous organizations are discussed, followed by a case study of one prominent distributed ledger technology, Bitcoin in chapter four.

3.2 Contracts

The Legal Information Institute [LII] of Cornell Law School¹¹ defines a contract as “*an agreement between private parties creating mutual obligations enforceable by law*” (Kim, 2017). It is effectively an arrangement with the essential characteristic of a bargain. For a party to be able to enforce a contract, five components need to be part of the agreement:

- **Adequate Consideration:** “*Something bargained for and received by a promisor from a promisee*” (Legal Information Institute, 2019a), such as an act or some form of property.
- The parties need to have the **capacity** to meet the requirements to enter a contract, which for example is not the case for minors or someone without soundness of mind (Legal Information Institute, 2019b).
- The agreed upon contract must be **legal** under the applicable governing law.
- It must be proven objectively (for example via notary) that both parties **agreed mutually** to any given contract via display of an offer and the acceptance of said offer.
- The promisee’s **offer**, be it “*to the benefit of the promisor or to the detriment of the promisee*” (Kim, 2017), is **accepted** by the promisor.

Additionally the participants in a contract are required to be willing and free to agree they are entering a legal relation between each other. In this context, business agreements are commonly accepted to be legally binding, while a social agreement, for example the

¹¹ <https://www.law.cornell.edu/>

promise to attend a birthday party, does not allow the host to sue the guest for not showing up. The law covering acts of civil wrongdoing disputes is named Tort law.

Contracts can be committed either in writing or orally via conversation. In case of a dispute though, it will be more difficult for a court of law to verify contractual obligations arranged between parties if they have not been converted into writing. An example for an enforceable oral contract is the visit of a baker and the purchase of a loaf of bread: even though no written contract is in place, the client's choice and order of a particular loaf requires her to pay the shop owner the prescribed price for this loaf. In certain scenarios, e.g. purchasing or selling land, a written contract document is required to confirm the transaction and update the land title register accordingly.

In case of a dispute a number of different options exist in order to resolve contractual complaints in and out of court. The European Commission for example has built an extensive framework for alternative dispute resolution [ADR] (European Parliament, 2013). Options under this scheme include mediation, conciliation, ombudsmen, arbitration and the complaints board. The principle behind these ADR procedures is to supply an easy, fast and inexpensive way to resolve contractual disagreements without having to take the litigation to court. This is a suitable approach for small financial disputes to avoid unnecessary costs, as various studies confirm. Saks (1992) found that “*delivering \$1 in compensation cost \$2.33*” (ibid, p. 1282) after 1985 in tort litigation results.

Trubek et al. (1983) support the notion of expensive small litigation cases and found evidence indicating the total legal fees for incidents seeking to recover less than USD 10,000.00 to exceed the net amounts recovered through court action. Their data also provided insight that in cases where plaintiffs recovered more than USD 10,000.00 the total legal fees would be a much smaller percentage of the recoveries. In the light of these costs, even some corporations set down in their policy statements to look first for ADR resolution before pursuing full-scale court litigation (Levin & Colliers, 1985). A more recent overview for median costs of litigation is provided by Hannaford-Agor (2013) and summarized in Figure 17.

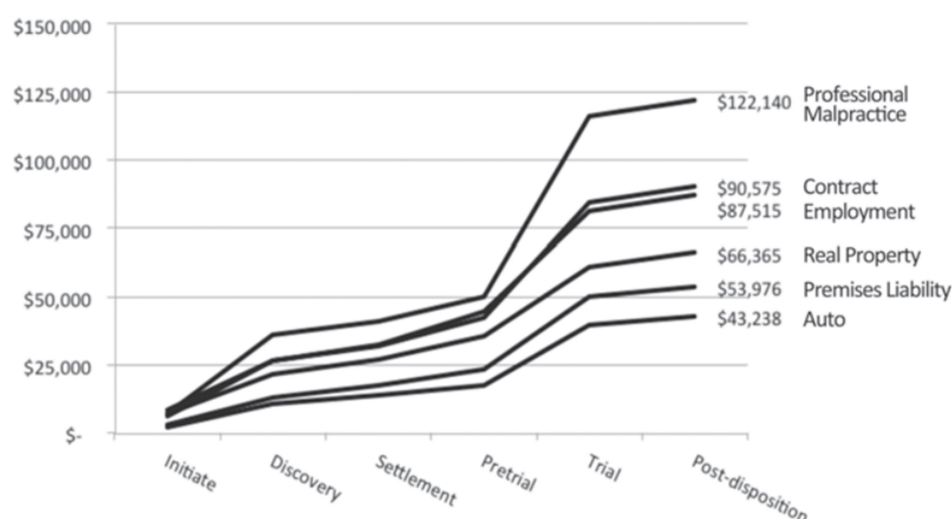


Figure 17: Median Costs of Litigation by Case Type (Hannaford-Agor, 2013, p. 26)

Figure 17 and the median costs are the result of a survey among members of the American Board of Trial Advocates [ABOTA] with 202 complete and 110 partial survey responses in August 2012. Median litigation costs rank second highest only topped by professional malpractice litigation. According to statistics of The World Bank¹² the average time for contract enforcement and resolving commercial disputes in local first instance courts in May 2018 took 582.4 days and resulted in costs of 21.2% of the claim value for OECD high-income countries¹³. Enforcing contracts is a costly undertaking and warrants improvement to reduce these expenditures as well as finding new solutions to avoid contract enforcement through courts.

These time-frames and costs pose a massive risk for clients of financial institutions in case of a banking failure. They are not necessarily able to enforce their contract due to limited resources on their side while the bank unilaterally changed the contract by failing or depositing toxic assets in an off-balance-sheet structured solution, such as a bad bank (Brenna, et al., 2009). A bad bank is defined as “*a bank that takes assets that have lost their value and debts that are unlikely to be paid back from other banks or organizations and deals with them in order to help with economic problems*” (Cambridge Business English Dictionary, 2019).

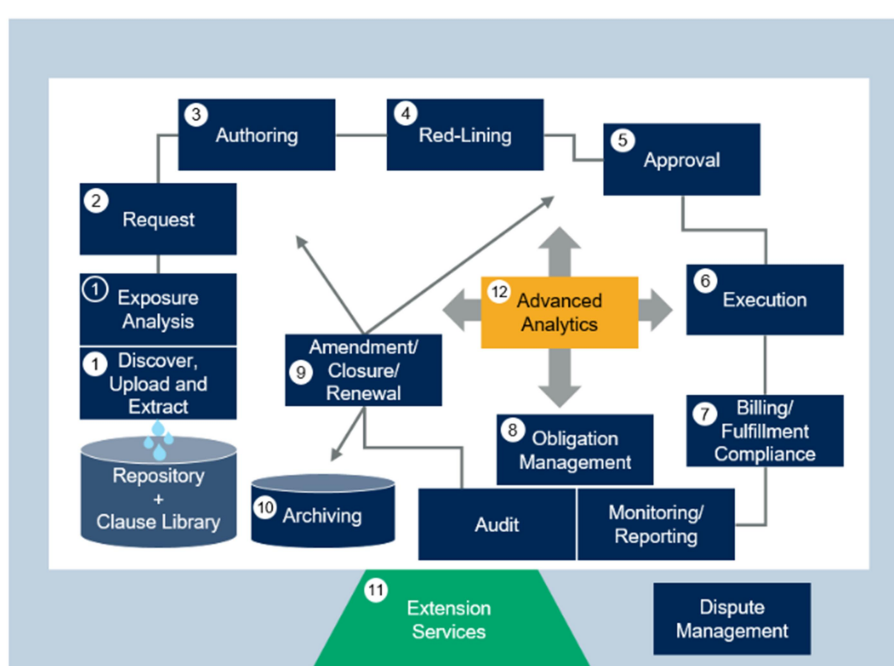
¹² <http://www.doingbusiness.org/en/data/exploretopics/enforcing-contracts> [accessed 14. April 2019].

¹³ The OECD defines 33 countries as of July 2018 as high income countries based on their previous four year (2014 to 2017) GNI per capita of more than USD 12,000.00 <https://www.oecd.org/trade/topics/export-credits/documents/oecd-export-credits-prevailing-list-of-countries-repayment-terms.pdf> [accessed 14. April 2019].

In a technological context, contracts are built and managed through specialised software solutions. These solutions will be briefly discussed in the next section.

3.3 Contract Management

From an information management perspective, financial institutions¹⁴ are likely to employ a contract life cycle management [CLM] solution (Sommers & Conaughton, 2018) responsible for managing all aspects of a contract: initiation, award, compliance and contract renewal. The typical workflow for such a piece of software is illustrated in Figure 18.



In a next step, from a vendor perspective, the collected details will be transferred into the order management and invoicing system, in order to drive automated contract compliance and to deliver the necessary documents for payments to the buyer.

These solutions are delivered in two flavours: either as an on premise installation that requires the use of local data repositories, such as a database, or alternatively as a peer-to-peer network based Software as a Service (SaaS). One such cloud based software is Contract Logix Premium, provided by the vendor contractlogix¹⁵. The software uses the infrastructure and platform services provided by Microsoft through its platform Azure¹⁶. In this scenario the end user relies on data security mechanisms provided by Microsoft and implemented through contractlogix. Microsoft has obtained global ISO standard certifications (for example: ISO 27001 on information security management; ISO 27017 on information security controls; or ISO 22301 on business continuity management) and with correct implementation through contractlogix guarantees contract data continuity. Data is supposed to be kept tamper resistant through the usage of AES 256 bit encryption for data at rest as well as TLS 1.2 data transfer encryption.

Despite these technological means, the central problem of information asymmetry remains and a contract management solution does not prevent information to be mismanaged. Thus, Blockchain based smart contracts will be explored as an alternative way for information management in the following.

3.4 Blockchain based Smart Contracts

The basis for improving current contracts between individuals and financial institutions is to remove the existing information asymmetry as well as the four factors of information mismanagement: data loss, data falsification, data misinterpretation and secrecy (Figure 1). In order to so, the ledger (which is currently a database) needs to be permanent (to prevent data loss), transactions immutable (so they are tamper proof), stored across multiple locations (to guarantee resilience) as well as removed from a central controlling entity (for example a financial services firm). This can be achieved via available fast connectivity on peer-to-peer networks, as well as advances in cryptography being part of the fifth industrial revolution (Perez, 2010). The concept finds its implementation and synthesis in the distributed ledger technology of which Blockchain technology is a subcategory.

¹⁵ <https://www.contractlogix.com/products/premium-clm/> [accessed: 3rd of April 2019].

¹⁶ <https://azure.microsoft.com/en-gb/> [accessed: 3rd of April 2019].

3.4.1 Blockchain Architecture

Christidis & Devetsikiotis define blockchain as „a distributed data structure that is replicated and shared among the members of a network” (Christidis & Devetsikiotis, 2016, p. 2293). It is a system of a digital, public and distributed ledger combining two concepts, BitTorrent peer-to-peer file sharing and a privacy system based on public-private key cryptography (Swan, 2015). The original idea was proposed in a whitepaper by an unidentified entity with the pseudonym Satoshi Nakamoto (2008) in context of the digital currency Bitcoin. In order for the digital currency system to work, Nakamoto proposed to establish a system utilizing cryptographic proof *rather than* trust in an intermediary to build a chain of digital signatures that can be verified by all members of the network for ownership authentication. Nakamoto’s concept, though, was not an entirely new one: already in 1983, David Chaum proposed an automated payment system enabling “individuals to provide proof of payment” (Chaum, 1983, p. 199) as well as preventing fraud by others (Chaum, et al., 1988) and later unsuccessfully tried to realize this potential with his company DigiCash (Pitta, 1999).

The Blockchain is a list of transactions (a log) batched together and supplied with a timestamp. They contain an account of all transactions similar to a public ledger (Lee Kuo Chuen, 2015). Each of these batched transactions is considered an individual block, can be identified through its cryptographic hash and contains a reference hash to its previous Block¹⁷. As Figure 19 demonstrates, the initial block of a new Blockchain is considered the genesis block.

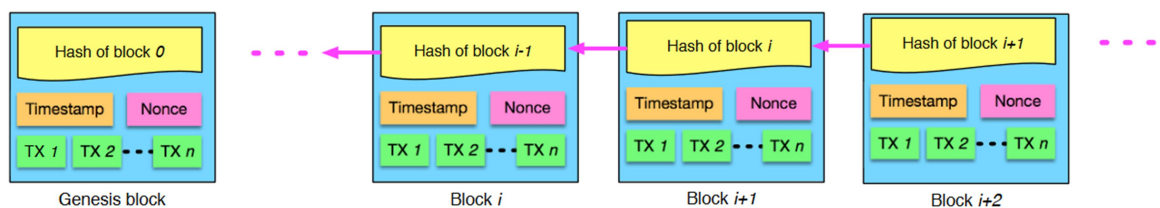


Figure 19: A sample Blockchain (Zheng, et al., 2018, p. 4)

Additionally, every block consists of the following two parts: a *block body* and a *block header* as demonstrated in Figure 20. The block body consists of the actual transactions included in the block, as well as a transaction counter. Depending on block size and transaction size, each block can contain more or less transactions.

¹⁷ Also: parent block.

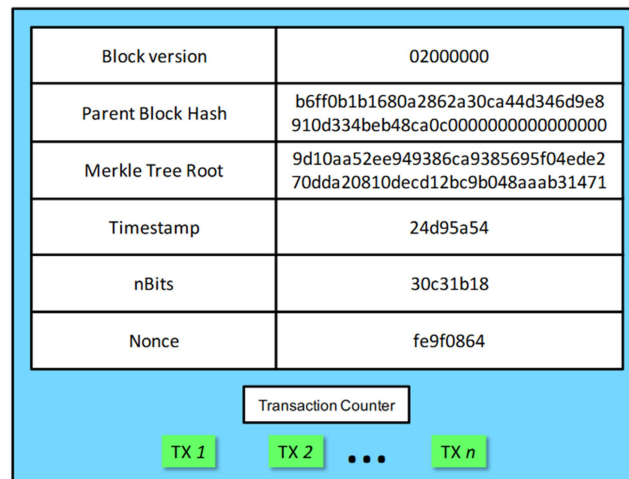


Figure 20: Example of a Block structure (Zheng, et al., 2018, p. 4)

The block header on the other side includes the block version, the parent block hash, the merkle root hash, a timestamp, nBits, as well as a Nonce (Lee Kuo Chuen, 2015).

- The **block version** number specifies which software version was used to generate this specific block.
- The **parent block** hash value is a 256-bit hash value indicating the previous block on the block chain.¹⁸
- The **merkle root hash** value summarizes all hashes associated with the different transactions within the block as an indirect hash. The amount of effort required for the creation of the merkle root hash is independent of the amount of transactions contained within the block.
- The **timestamp** reflects the time at the point of creation of the block “as seconds since the first of January 1970 UTC (coordinated universal time)” (Lee Kuo Chuen, 2015).
- The **nBits** (alternative name: “*difficulty target*” (Morabito, 2017)) area reflects the “*current hashing target in a compact format*” (Zheng, et al., 2018, p. 355).
- The **nonce** (alternative name: proof of work by miners (Morabito, 2017)) value is a number that “*is manipulated by the publishing node to solve the hash puzzle*” (Yaga, et al., 2018, p. 16) in a blockchain network utilizing mining.¹⁹

¹⁸ This is empty in the genesis block as there’s no parent block.

¹⁹ If the Blockchain network is not employing a mining procedure, they may or may not reference a nonce value. If they do, it is for a different purpose than the solution to a hash puzzle.

Along the chain, the blocks are ordered linear and chronologically. The block containing the newest transactions will always be added to the end of the chain. Each member of the Blockchain network (a so called node) holds a full copy of the Blockchain. This public ledger being available to every node removes the need for trusting transaction partners or requiring a (human) intermediary to validate and confirm the transaction (Swan, 2015). This decentralized peer-to-peer distributed network storage of the full ledger also increases the systems resilience, as it does not succumb to a single point of failure compared to a central database requiring additional work to achieve the same level of resilience already built into the Blockchain system (Figure 21).

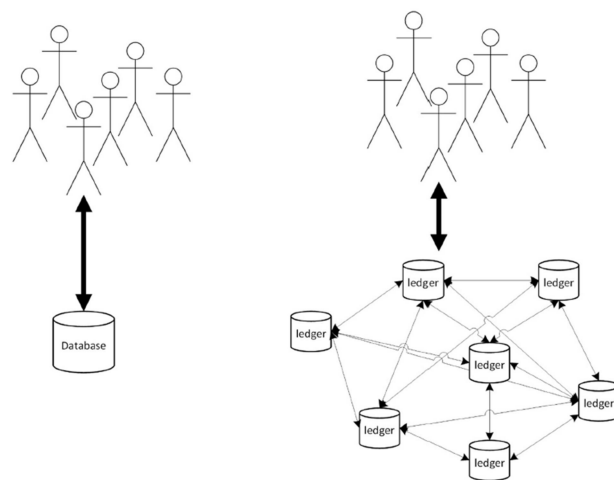


Figure 21: Schematic comparison: traditional database vs. public ledger (Ølnes, et al., 2017, p. 358)

There are three types of Blockchain system categories (Zheng, et al., 2017):

- A **Private Blockchain** is entirely controlled by one organization running a centralized Blockchain network. This central entity grants or withdraws access to the network, and it also most likely controls the final consensus decision. On one hand, due to the limited number of participants (contrary to a public system), a Private Blockchain is less tamper resistant because compromising individual nodes leads to larger control over the network. On the other hand, this lower amount of member results into a more efficient network that acts faster.
- A **Public Blockchain** allows everyone with the necessary soft- and hardware to join the system and fully access all records. As a decentralized set-up it is more difficult to interfere with transactions by compromising individual nodes, but processes and transaction throughput will be low due to the large amount of network nodes.

- As an illustration, a **Consortium Blockchain** is represented in the company R3, an association of banks and financial institutions developing the Blockchain called Corda for complex transaction handling in the world of finance (Guo & Liang, 2016). Similarly to a Private Blockchain, this type of system is less tamper resistant than Public Blockchains, but at the same time should be more network-efficient depending on the amount of nodes present.

Figure 22 illustrates the three different categories and ranks them on a horizontal axis from most decentralised to most centralised system. The permissionless public shared system equals the public Blockchain; the permissioned, public, shared system equals the consortium Blockchain and the permissioned, and the permissioned, private, shared system falls in the private Blockchain category.

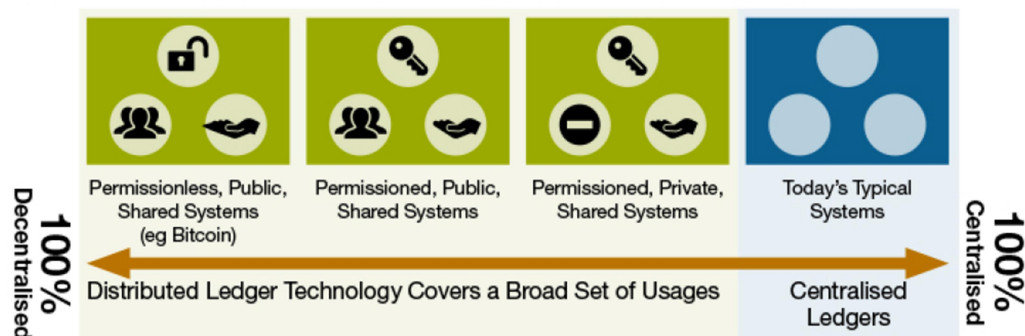


Figure 22: Degrees of centralization in different DLTs (Walport, 2016, p. 35)

The peer-to-peer network on which a Blockchain is based upon requires four steps to be operational:

- The users employ asymmetric-key cryptography²⁰ to generate a public and private encryption key (Romine, 2013). The public key is being made available for every participant in the network to use, while the private key remains concealed with the original creator²¹. In the situation of a transaction (Figure 23), the user "Alice" runs a hash process over her transaction log; applies her private key to encrypt the hash and sends a package, combining both, her transaction, as well as the encrypted hash to "Bob" for verification.

²⁰ This can also be referred to as public key cryptography.

²¹ While there is a mathematical relation between both keys, the knowledge of the public key is not efficient to determine the nature of the private key.

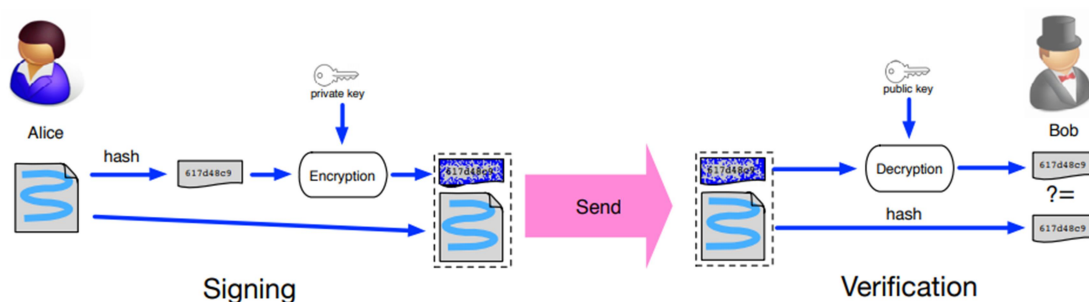


Figure 23: Example of a digitally signed transaction (Zheng, et al., 2018, p. 5)

- Bob in turn makes use of Alice's public key to decrypt the hash Alice sends, as well as in turn hashes Alice's transaction himself²². Should the two hashes, the one decrypted with Alice's public key, as well as the one created by Bob via hashing Alice's transaction himself, be identical, then Bob verifies Alice's transaction. The advantage of this method for digital signatures is that it brings integrity (Christidis & Devetsikiotis, 2016) to the network allowing non-trusting parties to interact without the need of a trusted intermediary.

The example in Figure 23 is a simplification of the validation process, as not only Bob would verify Alice's transaction, but rather all of Alice's neighbouring peers would ensure the validity before relaying the information even further.

- Following a pre-determined time interval, the network does validate and collect all executed transactions, structures them and finally collates them into a candidate block receiving a timestamp. Commonly, this process is referred to as mining and the mining node sends the completed block back into the network to be attached to the Blockchain.
- Subsequently, all network participating nodes verify that the candidate block contains only valid transactions and correctly references its parents block's hash. Once both premises are fulfilled, the nodes add the newly mined block to their (local) chain. If they are not both realized, then the candidate block instead is discarded.

²² This system can also be practiced the other way around, encrypting a text via a public key before sending it to the owner of the associated private key for decryption. It is typically used in encrypted email exchanges, for example between security researchers or reporters and their sources. Pretty Good Privacy (PGP) is an example of a piece of software allowing email encryption via asymmetric key encryption.

All four steps are illustrated in this flowchart:

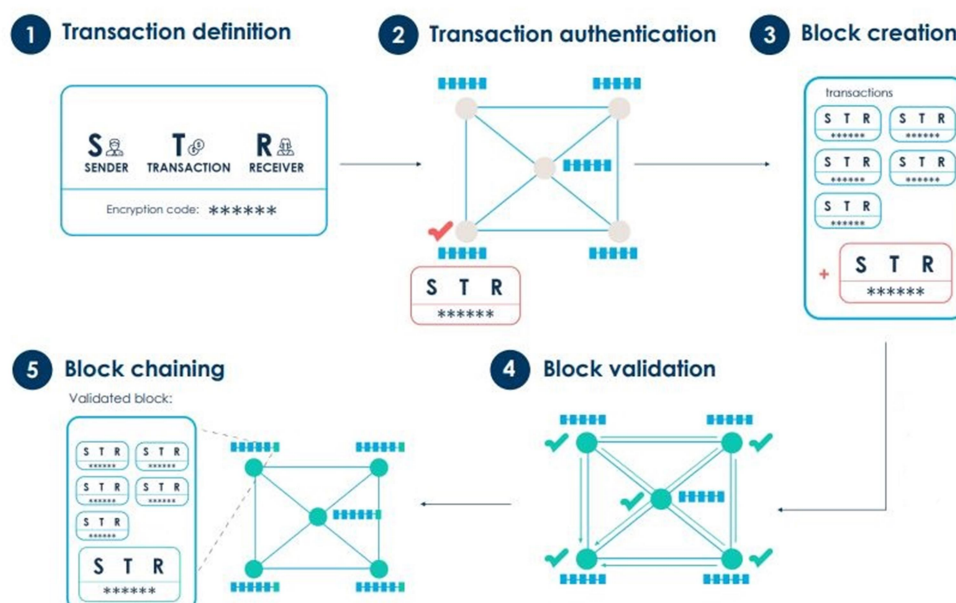


Figure 24: Process of Block creation (Froystad & Holm, 2015, p. 10)

For the provision of their computing resources to the Blockchain network, the participating nodes receive a reward if they successfully propose the next Block to the chain. This reward takes the form of the network account units (e.g. Bitcoins for the Bitcoin network) either provided as transaction payment or as an “*ex-nihilo creation*” (Houy, 2016) inherent to the Blockchain platforms technology.

It is possible for a technical glitch (Swanson, 2015), a so called fork, to occur during this process: since block validation happens independently from each other at various nodes simultaneously, it is possible that concurrently two or more different Blockchain branches²³ exist with different sets of included transactions (Tschorsch & Scheuermann, 2016). In such a scenario the ownership in transactions is not clear and the system will try to resolve the fork: within the Bitcoin network for example, the mining process is advanced on the local chain involving the highest amount of computational effort (ibid.). Following this procedure, there will be a point in time when one forked Blockchain branch will overtake the other(s) and become the representation of the largest accumulated computational effort. In Figure 25 below this “*heaviest*” (Eyal, et al., 2016, p. 47) branch is the one containing the letter B blocks, while the letter G blocks branch is orphaned, classified as not to be worked anymore and discarded by the network.

²³ A branch is the continuation of a Blockchain resulting when multiple miners create different blocks and attach them simultaneously to the same parent block.

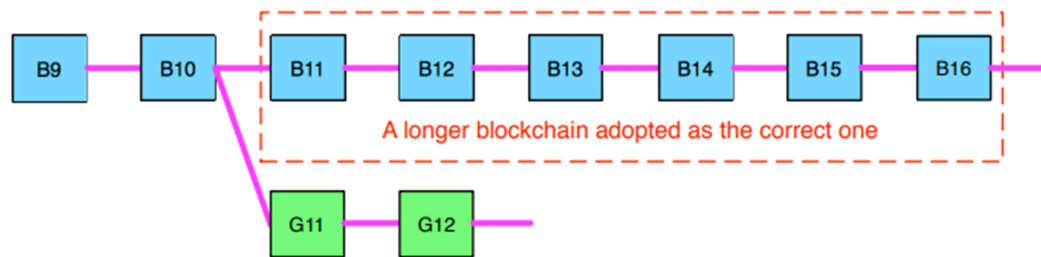


Figure 25: Example of forked Blockchain branches (Zheng, et al., 2018, p. 8)

Despite this procedure a risk of manipulation, for example a double-spending attack (illustrated in Figure 26) remains: a double-spending occurs if the malicious user Jim tries to spend the same amount of currency with a vendor and at the same time with a fake user Jimmy (that is controlled by Jim), sending both transactions to two different subsets of mining nodes, thus leading to Blockchain branches via forking (Natoli & Gramoli, 2016). In this scenario, Jim tries to obtain the vendor's goods without paying for them, as he expects the branch

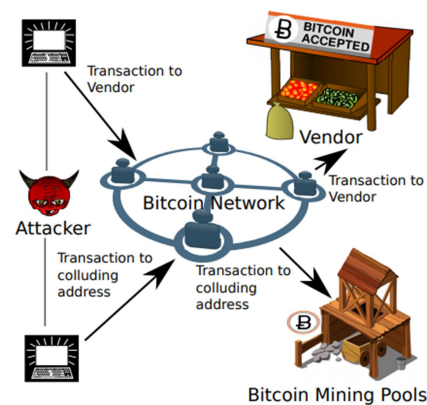


Figure 26: Sketch of a double-spending attack (Karame, et al., 2012, p. 909)

3.4.2 Consensus Mechanisms

Contrary to the traditional approach of transaction ratification via a trusted third party (e.g. a bank), the Blockchain concept has the trusted middleman built into the network already. Figure 27 details a classical interaction between a customer and a vendor in which two banks are playing the role of the trusted intermediary to endorse the customer's ability to pay for a transaction with the vendor – for example a purchase at a local clothing store.

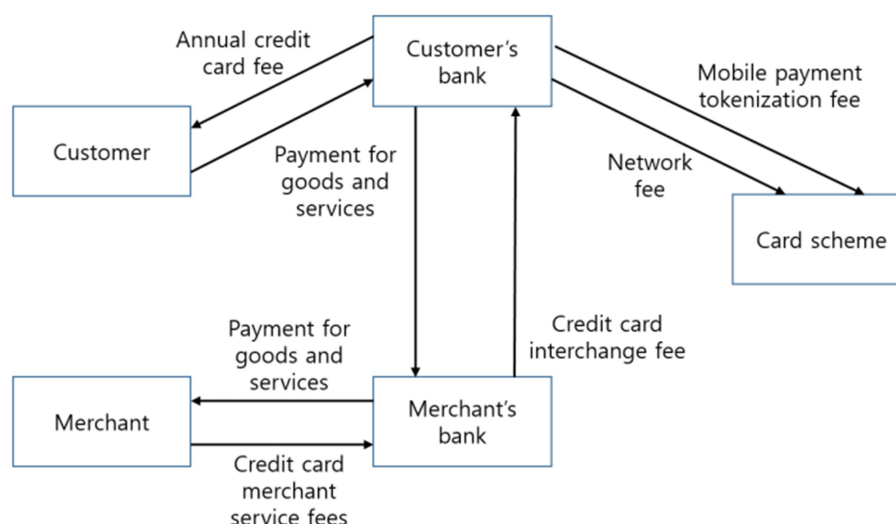


Figure 27: Trusted 3rd party interaction (Park & Park, 2017, p. 8)

In this illustration, the client pays an annual fee for her credit card and in return is able to pay the merchant via her bank and the merchant's bank. Fees occur for the transaction between both banks on the client's side, as well as on the merchant's side for the banks services.

In a decentralized network with no central authority, the approach depicted above does not apply. Thus a different mechanism must be used to achieve trust among the anonymous members of the network. In order to do so, a solution to the *Byzantine Generals Problem* for reliable computer systems (Lamport, et al., 1982) must be found.

The Byzantine Generals Problem is a thought experiment portraying the difficulties in making decisions for a Byzantine army about to attack. Within the army, platoon leaders and generals cannot be sure if a traitor is among them and thus must find an effective way to coordinate their attack and not set themselves up for failure (ibid.).

The various Blockchain software pieces commonly offer five major and different consensus mechanisms to solve the Byzantine Generals Problem and guarantee trust to the network members. The consensus mechanisms can either be permissionless,

allowing “*everyone in the world*” (Zheng, et al., 2017, p. 559) to participate, or permissioned in which case the authority responsible for the Blockchain has to give a new user permission to join the network. All five instruments of consensus are defined by eight basic parameters which can vary in their specific application depending on the consensus mechanism in place (Seibold & Samman, 2016):

- **Authentication:** A participants identity needs to be verified;
- **Decentralized governance:** There is no central facility to provide authority over transaction completeness;
- **Fault tolerance:** Individual server or node failure will not affect the network efficiency;
- **Integrity:** The transaction validity is enforced through hash sum comparison.
- **Nonrepudiation:** A way to ensure “*irrefutable evidence regarding the transfer of a message from the originator to the recipient*” (Zhou & Gollmann, 1996, p. 55);
- **Performance:** The software considers the networks physical limitations, such as scalability or throughput;
- **Privacy:** The system guarantees that only intended recipient and originator can read and access the transaction; and
- **A quorum structure:** A set of rules protecting “*the consistency and availability of replicated data despite the benign failure of data repositories*” (Malkhi & Reiter, 1998, p. 203).

Additionally consensus protocols need to be

- **consistent**, so that all consensus makers only make decisions that are final and contain the same value;
- **valid**, as in the final value was originally put in by one of the consensus makers; and
- **wait-free**, so that agreement is reached within a limited quantity of steps (Barborak, et al., 1993).

The five major consensus mechanisms applied by different Blockchain software packages are the following:

- **Proof of Work [PoW]:** The PoW framework requires participating network nodes to vote for attaching a specific, newly created Block to the current branch via the provision of computing capacity (mining) in order to solve a mathematical puzzle and for example find a new hash value smaller than the nonce in the current parent block (Gervais, et al., 2016). If a mining node has found a Block fulfilling this requirement, it broadcasts its Block and hash value to its peers for verification.

The advantages of this system are its openness as everyone with hardware to solve the puzzle can attempt doing so, as well its resilience against Denial-of-Service (DoS) attacks. The latter attempts to flood the network with false Blocks, which is made impossible as only Blocks with the required nonce values will be accepted by the network. On the negative side, the computationally intensive design of this consensus system leads to high levels of electricity consumption (O'Dwyer & Malone, 2014), thus negatively impacting the global carbon dioxide emission (Becker, et al., 2013). A second risk is posed through a consortium of mining nodes (Kroll, et al., 2013) controlling more than 50 percent of the Blockchain's computing capacity to solve the hash puzzles. This majority ownership would allow the conglomerate for example to change consensus rules, censor transactions or perform malicious double-spending. Proof of Work is currently implemented in the majority of Blockchain software packages (Gervais, et al., 2016) and common for permissionless Blockchains.

- **Proof of Stake [PoS]:** Since Proof of Work consensus is considered to waste a noteworthy amount of energy (Watanabe, et al., 2016), an alternative method of achieving consensus, Proof of Stake, is being explored to reduce the energy dependency of Blockchains (King & Nadal, 2012): instead of network nodes investing their computational resources into solving mathematical challenges, the idea of PoS evolves around the idea that those nodes that are more invested into the Blockchain network will be more likely to support the success of the network and less likely to sabotage it (Yaga, et al., 2018). The investment in this scenario is the amount of cryptocurrency (the stake) any given user holds as part of the network. Four approaches on how a Blockchain can treat a stake are: coin aging systems, delegate systems, multi-round voting and random selection of staked users (ibid.).
 - **Coin aging systems**, also **coin age PoS**: these refer to the age feature of a staked cryptocurrency in order to allow a node with a higher stake to publish more blocks to her branch of the Blockchain. Each coin has a cooldown timer attached to it, and is being triggered whenever the owning node uses it to create and publish a new Block, so that this stake cannot be used to publish another Block until the cooldown has ended. The older and more substantial the measure of cryptocurrency coin a given node is holding, the more likely it is chosen to publish the next Block. With regards to stockpiling older cryptocurrency coins in pursuance of higher influence over the network, the system contains an inherent maximum probability of

- winning: once this maximum is reached, older and more coins will not make it more likely for the node to win the race for the newest collection of transactions.
- **Delegate Systems**, also **Delegate PoS**: under this scheme all network participants are voting for some among them to become publishing nodes (or miners) responsible for verifying transactions and bundling them into new Blocks (Kiayias, et al., 2017). The voting procedure is continuous and in similar fashion to granting publishing rights to a node, a negative quorum will result in the withdrawal of this publishing right. The risk of broadcasting right recall and associated reputation as well as rewards incentivizes positive behaviour of the elected agents. In this context each user's stake is used to weigh their voting ability (Xu, et al., 2017).
 - **Multi-round voting**: based for example on the coin aging system, the Blockchain network selects several nodes based on their user's stake in the network to allow them to publish Blocks (Li, et al., 2018). Afterwards all staked members of the Blockchain fabric vote which nodes proposed Block should be published. Ultimately this might require more than one round of voting, hence the naming convention.
 - **Random selection**: occurs if the utilized system chooses a new publishing node pseudo-randomly based on the ratio of their individual stake to the overall available total stake of the Blockchain organization (Ferreira Jesus, et al., 2018). If a node holds 15% of the full network stake, it would be chosen 15% of the time to publish a new Block. This type of Proof of Stake is also sometimes defined as chain-based PoS.
- **Round Robin [RR]**: This consensus mechanism is typically put to use in permissioned Blockchain structures, as it pre-supposes trust among network participants which cannot be guaranteed in permissionless systems. RR, originally stemming from distributed systems research (Yaga, et al., 2018), requires that all network participating nodes take turns in being miners. This way, it is ensured, that an individual stakeholder creates the majority of new Blocks. Figure 28 briefly illustrates the RR concept for a 6 node set-up below.

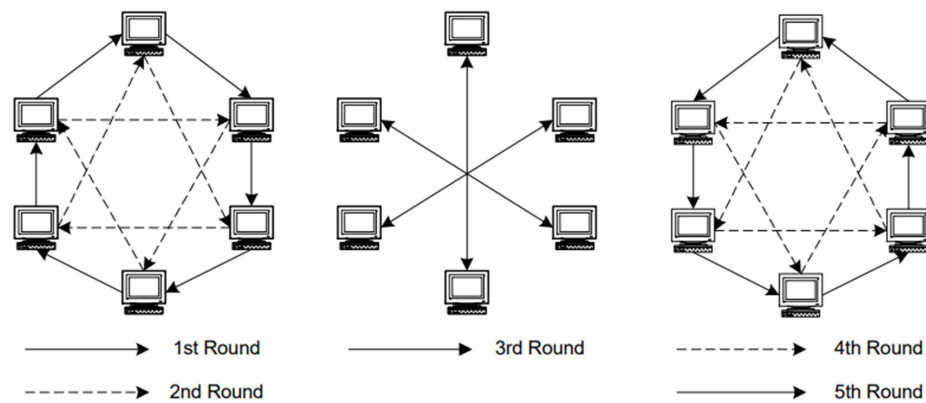


Figure 28: Round Robin with 6 participating nodes (Ranganathan, et al., 2001, p. 9)

- Proof of Authority [PoA]:** this algorithm relies “on a set of N trusted nodes called the authorities” (De Angelis, et al., 2018, p. 3) acting as publishing nodes for new Blocks and being verifiably linked to real-life individuals or organizations (Yaga, et al., 2018). The system assumes that all network users constantly evaluate the behaviour of these miners, which, based on the evaluation, either gain or lose reputation. The higher any given miner’s prestige, the more likely it is to be able to publish the next new Block. Due to the requirement for identified node owners acting as publishing nodes, this consensus mechanism is only implemented in permissioned Blockchains.
- Proof of Elapsed Time [PoET]:** underlying this consensus concept is the idea that each publishing network member runs specific, trusted hardware²⁴ (Dinh, et al., 2018) generating random timers with randomly selected time intervals to keep the node idle (Eyal, 2017). The miner which’s idle state finishes first, will disclose the next Block to the network and every other miner still idling, will awake from its sleep so the process may begin anew.

In distinction to these five major consensus algorithms, various other computational processes to achieve harmony on a Blockchain network exist: for example Proof of Burn [PoB] or Proof of Capacity [PoC] (Chalaemwongwan & Kurutach, 2018). Similar to the five major mechanisms, the aim of these other protocols is to reduce computational power requirements and usually to apply to specific use cases, instead of the more widely applicable major consensus mechanisms.

²⁴ Examples of this are Intel’s SGX and AMD’s Secure Technology platforms.

Other Blockchain application scenarios outside Finance (Treleven, et al., 2017) can be found in:

- **Education** as a digital record of intellectual achievement in order to reduce qualification fraud for example in job applications (Sharples & Domingue, 2016).
- **Government**, for example as an enabler of digital government initiatives for electronic voting (Ayed, 2017).
- The **Internet of Things** [IoT] (Conoscenti, et al., 2016): in which Blockchain applications might process sensor data automatically, allow devices to communicate with each other and autonomously execute tasks (e.g. turn on the water heater 15min after a homeowner started her car in the evening on a workday to provide her with hot water for a shower after her 40min commute home).
- **Insurance**, where they should be able to speed up claims processing (Gatteschi, et al., 2018).
- **Intellectual Property**, for example through Non-Disclosure Agreements [NDA] (de la Rosa, et al., 2016), “*decentralized trusted timestamping*” (Schönhals, et al., 2018, p. 108) or Digital Rights Management [DRM] and Conditional Access Systems [CAS] (Kishigami, et al., 2015). The information stored on the Blockchain serve as certification of existence and reference to the idea's/document's author.

3.4.3 Smart contracts

Smart contracts are part of the Blockchain version 2.0 (Swan, 2015), the technology advance that followed after the initial Blockchain concepts utilizing cryptocurrencies for payments between anonymous parties without trusted middleman, and one step before decentralized autonomous organizations [DAOs] (Figure 29).

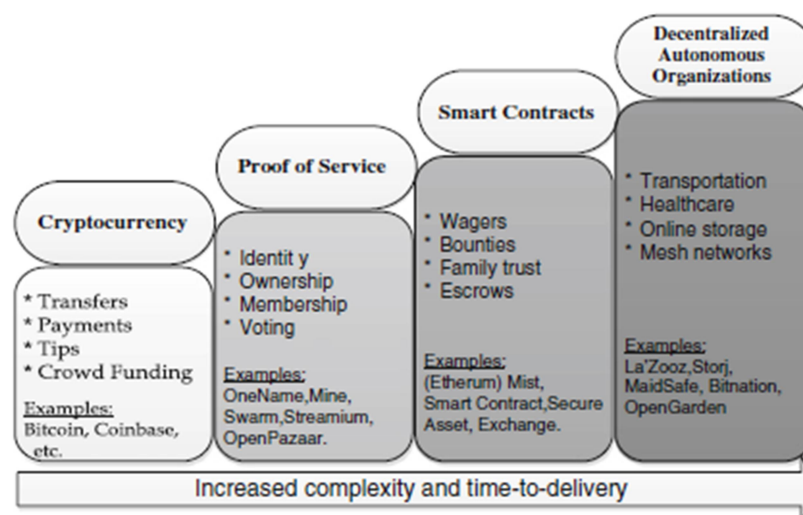


Figure 29: Blockchain technology subdomains (Morabito, 2017, p. 32)

The concept of a smart contract was first introduced (Christidis & Devetsikiotis, 2016) by Nick Szabo²⁵ as “a computerized transaction protocol that executes the terms of a contract” (Szabo, 1994). He proposed to rewrite contractual definitions, for example “delineation of property rights or collateral” (Szabo, 1997), into machine code and embed them into soft- and/or hardware to reduce the requirement for intermediators and the manifestation of accidental or malicious anomalies potentially requiring legal intervention to be resolved.

According to Szabo (ibid.) a smart contract is not dissimilar to a vending machine: each user of the machine is entering into a contractual exchange with the apparatus; currency is entered by the user, the machine dispenses change and the chosen product based on the displayed price. The automaton's till is encased in a lockbox and the overall machine is protected through hardened material as well as other security mechanisms in order to ensure a burglar's requirements to penetrate the system are more costly than the contents of the cash register (Szabo, 1997).

²⁵ According to the New York Times, Szabo might have worked as a contractor for David Chaum's firm DigiCash for a couple of months (<https://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html>).

Algorithmic trading can be considered another example of a smart contract (Kölvart, et al., 2016): computer to computer trading has consistently been on the rise²⁶ while strictly human to human trading has declined (Chaboud, et al., 2014). The utilized software in this automated market is slightly different from Blockchain Technology, as it relies on centralized SQL databases, but similar to a smart contract, these trading programs act autonomously when specific events occur.

In the context of Blockchain technology, a smart contract is “*a program that runs on the Blockchain and has its correct execution enforce by the consensus protocol*” (Luu, et al., 2016, p. 254). In this, it is similar to stored procedures in a relational database (Christidis & Devetsikiotis, 2016), which, given a permitted user request, run and produce an output. Every smart contract is stored as a script on a suitable Blockchain protocol, for example Ethereum (Buterin, 2014) or Hyperledger (Androulaki, et al., 2018), and in order for the result of the smart contract to be valid, all executing members of the Blockchain network need to obtain the same conclusions when individually executing the smart contract. Any confirmed result will be recorded as valid transaction on the next published Block (Yaga, et al., 2018).

A more complex smart contract is the decentralized autonomous organisation. Such organizations²⁷ are defined as “*long-term smart contracts that contain the assets and encode the bylaws of an entire organization*” (Buterin, 2014). The objective of a DAO would be to transform conventional corporate governance into computer code in order to allow organizations broader scale and flexibility while maintaining formal corporate structures (Wright & De Filippi, 2015). In this fashion the decentralized autonomous organization could become the evolution of the publicly held business corporation Jensen & Meckling (1976) envisioned, in which agency costs could be reduced even further due to strict and unchangeable, software based contracts. Existing proposals for Blockchain based voting (Wang, et al., 2018) (McCorry, et al., 2017) indicate that it would be possible to allow DAO shareholders to participate directly and location independent in the organizational decision making as long as they are able to access the Blockchain network. This would remove the necessity for a central management authority steering the corporation, as well as lower operational costs. Accountability of all decisions as well as the business actions is automatically enforced since all transactions are secured through the Blockchain’s encryption and integrity mechanisms.

²⁶ Some estimates assume more than 50% of the European and North American equity trade.

²⁷ The American technologist and author Daniel Suarez gives a fictional example of a worldwide DAO in his two part novel series *Daemon* (2006) and *Freedom™* (2010).

In order to prevent banking failure in the future, a financial institution would have to be built following a decentralized autonomous organization blueprint in which the founders and future members of the corporation would be able to participate in and vote on the full decision making process. Due to the distributed ledger being available to every member in the network, information (for example about bad investment choices) could not be hidden from the public's eye, as every new participant would automatically receive the full ledger. Smart contracts would serve as the autonomous controlling mechanism, making sure to alert users to unsavoury behaviour or even directly removing their funds from the organization. This is visualized in Figure 6: all transactions of a bank are accessible via a public, permissionless ledger mitigating any type of information manipulation.

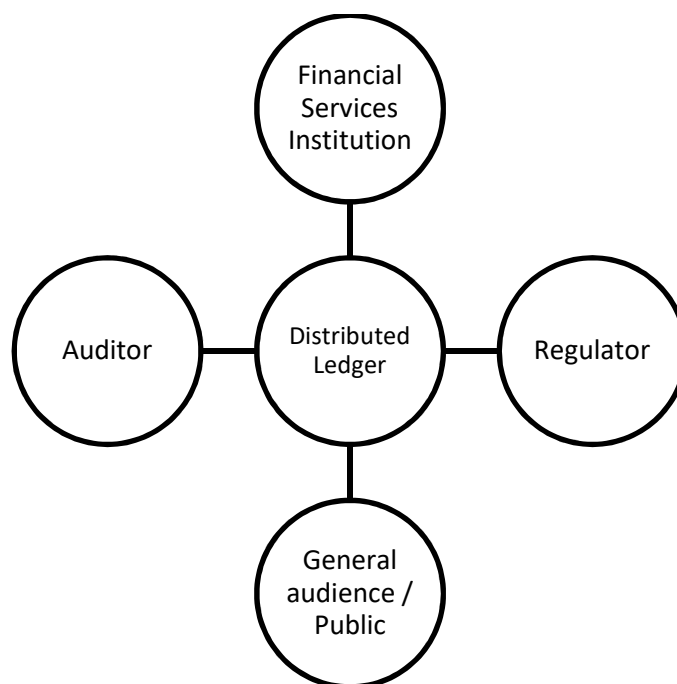


Figure 6: Simplified auditing process chart for distributed ledger

3.5 Conclusion

The technological viability of distributed ledger technology has opened up the pathway for changing the way businesses and organizations, but also individuals operate. Making transactions of any form transparent, but also immutable against retro-active change without consent from the transacting parties, as well as the participating network allows to conceptualize and to implement new organizational forms preventing mistakes from the past (as pointed out by Maull et al. (2017) in their flowchart below).

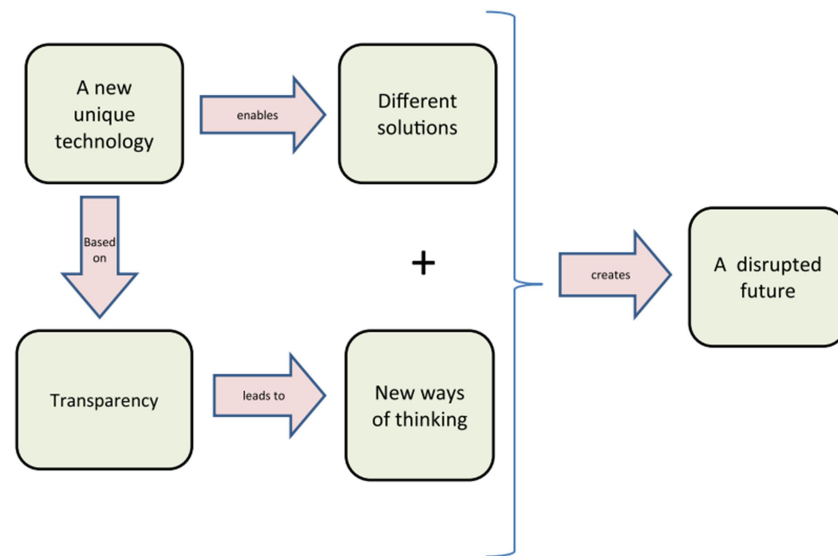


Figure 30: Distributed Ledger Themes (Maull, et al., 2017, p. 484)

Preventing information loss and mismanagement through a public Blockchain or likeminded technologies while also granting access to the same information to every interested party, will act as an effective governance tool to supervise organizational behaviour. Adding the capability of legally viable, automated smart contracts enacting specific, pre-agreed transactions immediately upon perceiving a pre-defined trigger (such as news headline), allows this governance to even be executed without manual intervention.

Moreover, with regards to legal requirements for a viable contract (adequate consideration, capacity, legality mutual assent, as well as offer and acceptance), the information symmetry guaranteed via the transparency of the distributed ledger will allow the contracting parties to verify the other parties claims and assurances.

In order for this potential disruption to current business conduct and governance approaches to occur though, the technology will have to be adopted widely in the four spheres: economic, political, social and technical (Woodside, et al., 2017). There exist advantages and disadvantages to distributed ledger technology adoption in these four categories, but two current obstacles to wider adoption are the political consideration of Blockchain based currencies as unregulated markets (ibid.), as well as concerns over the privacy and security of the technology (Li, et al., 2017) (Joshi, et al., 2018). One element of the first barrier is currently under revision of the U.S. Securities and Exchange Commission [SEC]: the Cboe BZX Exchange Inc. has petitioned the commission to allow the trade of a Bitcoin based exchange-traded fund [ETF] (Securities and Exchange Commission, 2019).

Implementation strategies and approaches are keys for every successful technology adoption especially with potentially far reaching consequences such as distributed ledger technology. It will require large scale government involvement for regulation of the systems and taxation of its associated currencies (Lehdonvirta & Castronova, 2014), as well widespread user adoption. Some of these factors will be discussed in chapter four in the Bitcoin case study.

Chapter 4 – Case Study: Bitcoin vs. Fiat Currency

4.1 Introduction

This chapter discusses Bitcoin's potential to be widely adopted for conducting business and transacting payments. It also analyses its impact on the environment through the network's energy requirements, as well as takes a look at the volatility between Bitcoin and fiat currency exchange.

4.2 Distributed Ledger Technology – Bitcoin

4.2.1 The Tragedy of the Commons and Bitcoin's Answer

The initial Blockchain 1.0 concept was proposed by an unknown entity with pen name Satoshi Nakamoto (2008) through a whitepaper detailing a solution how to possibly answer the tragedy of the commons problem in distributed networks. The tragedy of the commons, originally introduced "*in 1833 by a mathematical amateur named William Forster Lloyd*" (Hardin, 1968) and popularized by the U.S. American philosopher Garrett Hardin in a 1968 article published in Science, describes a thought experiment in which a common piece of land is shared by various cattle herders. Hardin continues to describe in his game theory concept how it would be advantageous for each herder to bring additional animals to the piece of land resulting in a situation in which, if all herders only considered their own economic situation, the common would be overgrazed and depleted to the economic detriment of the whole group of herders. The simplified situation of two herders 1 and 2 is graphically represented in Table 2. It is an application of the prisoner's dilemma (Tucker & Straffin Jr., 1983) to the tragedy of the commons situation.

Herder 1	Herder 2		
		Add more cattle	Do not add cattle
	Add more cattle	$(-1, -1)$ [B]	$(1, -2)$ [Γ]
	Do not add cattle	$(-2, 1)$ [Δ]	$(10, 10)$ [E]

Table 2: The prisoner's dilemma applied to the tragedy of the commons

The four values "-2, -1, 1 and 10" represent payoffs to the two herders within the game theoretical mind-set. If only one of the two herders adds additional cattle to the land, she will receive additional economic pay-off, while her counterpart will not (either " Γ or Δ ").

Assuming both herders are economically self-interested, they will anticipate that the other side will add cattle to the land and in order to not lose out themselves will also add cattle. This leads to situation “B”, which represents the tragedy of the commons in which the land is overgrazed. The favourable situation “E” will only be achieved if both participants do not set additional cattle to graze on the common land. According to Hardin, rational self-interest in context of shared, limited resources must lead in eventual depletion of said resources (Hardin, 1968).

Nakamoto argues that their proposed incentive scheme²⁸ and proof of work concept (for new Block creation “*may help encourage nodes to stay honest*” (Nakamoto, 2008, p. 4) as well as continue to contribute to the network and act in the networks favour. Further research following Nakamoto’s publication revealed, that this proposal would not be sufficient to avoid the tragedy of the commons problem (Pilkington, 2016) and that ultimately network participants, given enough computing resource accumulation (Bentov, et al., 2014) would only act in their self-interest. Thus, they would not be aligned with the benefits of the network any longer. Other distributed ledger technologies following Bitcoin’s lead have taken this into consideration and try to address the challenge with different consensus mechanisms.

Additionally to the weakness of Bitcoin’s proof of work consensus mechanism resulting from the tragedy of the commons (e.g. through a 51% attack (Bastiaan, 2015) (Saad, et al., 2019)), the technology and its associated cryptocurrency have fallen prey to two major and many smaller thefts in recent years: the Mt. Gox Bitcoin exchange hack in 2014 resulting in an estimated loss of USD 500 million (McMillian, 2014) and the Coincheck Inc. hack with an estimated loss of USD 530 million (Wilson & Wada, 2018).

Despite these circumstances, Bitcoin remains the most traded cryptocurrency and most popular DLT according to the rankings of Coinranking (Figure 31), Coinbase (Figure 32) and CoinMarketCap (Figure 33).

²⁸ The incentive structure in the Bitcoin network provides miners with Bitcoin currency for their efforts in providing computing resources to the network.






COINS	PRICE	MARKET CAP	24H CHANGE
1  Bitcoin	\$ 5,308.79	\$ 93.73 billion	1.29% +
2  Ethereum	\$ 173.52	\$ 18.23 billion	0.67% +
3  XRP	\$ 0.3307	\$ 13.88 billion	0.15% +
4  Bitcoin Cash	\$ 302.67	\$ 5.37 billion	1.55% +
5  Litecoin	\$ 81.04	\$ 4.98 billion	0.20% +

Figure 31: Coinranking screenshot (Coinranking, 2019a)











#	NAME	PRICE	CHANGE	MARKET CAP	CHART
1	 Bitcoin BTC	\$5,326.12	-40.23%	\$94.0B	 Trade
2	 Ethereum ETH	\$174.01	-71.91%	\$18.4B	 Trade
3	 XRP XRP	\$0.33	-62.04%	\$13.9B	 Trade
4	 Bitcoin Cash BCH	\$302.86	-74.23%	\$5.4B	 Trade
5	 Litecoin LTC	\$81.61	-44.82%	\$5.0B	 Trade

Figure 32: Coinbase screenshot (Coinbase, 2019)











#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	 Bitcoin	\$94,329,634,356	\$5,342.70	\$13,816,411,563	17,655,812 BTC	1.39%	 ...
2	 Ethereum	\$18,392,280,090	\$173.94	\$6,378,062,228	105,737,311 ETH	0.64%	 ...
3	 XRP	\$13,870,746,646	\$0.330486	\$966,714,234	41,970,748,057 XRP *	-0.22%	 ...
4	 Bitcoin Cash	\$5,381,854,930	\$303.40	\$1,221,058,152	17,738,688 BCH	1.54%	 ...
5	 Litecoin	\$4,998,797,626	\$81.38	\$2,604,057,805	61,422,984 LTC	-0.29%	 ...

Figure 33: CoinMarketCap screenshot (CoinMarketCap, 2019)

This popularity is supported by the acceptance of Bitcoin by global cryptoasset service providers (Figure 34). Almost all surveyed service providers support Bitcoin technology.

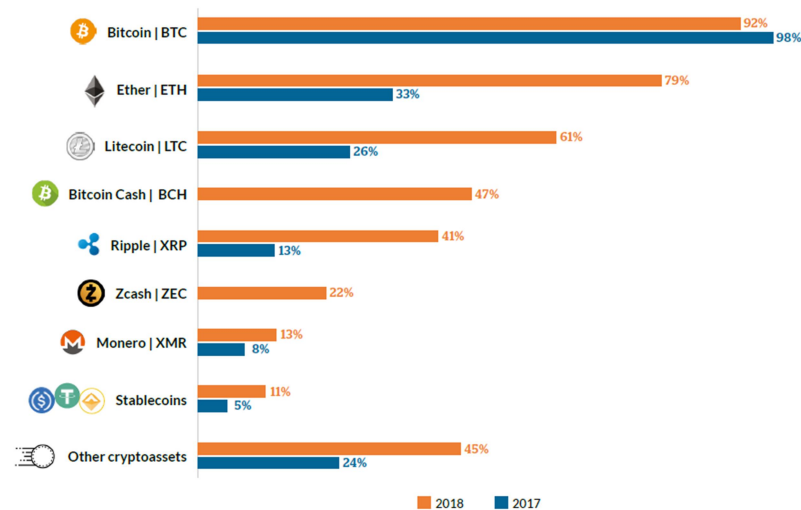


Figure 34: Service provider support for cryptoasset (Rauchs, et al., 2018, p. 30)

It is interesting to note though, that while Bitcoin dominates the monthly on chain transaction volumes, Ethereum, the second most popular technology according to the above rankings, is used much more often for payment processing (Figure 35).

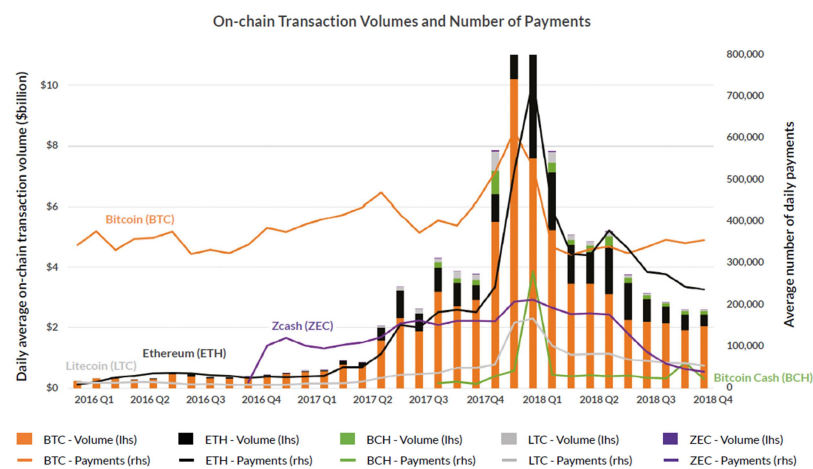


Figure 35: Transaction volumes and number of payments on multiple DLTs (Rauchs, et al., 2018, p. 37)

4.2.2 Conducting Business with Bitcoin

Considering Bitcoin's strength in payment processing, its technology adoption hinges on the availability of users being able to conduct business transactions via the network and being able to transform virtual currency into fiat money²⁹ (Swan, 2015) for example through high street automatic teller machines [ATMs].

According to the statistic published by coinmap.org, there are currently 14659 venues accepting Bitcoin for payments globally (Coinmap, 2019)³⁰. Utilizing the website's time bar reveals this number to be the result of a steady growth of businesses adding this functionality to their portfolio initially starting on the 26th of February 2013 with 3 venues to the current number on the 16th of April 2019. This acceptance growth is mirrored by the number of ATMs accepting cryptoassets being deployed (Figure 36), even though the two largest markets in this regard are North America and Europe in first and second place respectively (Coin ATM Radar, 2019c). The global amount of cryptoasset capable ATMs is estimated to be 4628 (Coin ATM Radar, 2019a).



Figure 36: ATMs accepting cryptoassets - net changes globally (Coin ATM Radar, 2019b)

²⁹ Fiat money is a currency which has been established typically through governmental regulation and often is without intrinsic value.

³⁰ According to the same data, there are at the moment 15 local businesses accepting payments in Bitcoin in the greater Dublin area.

In comparison, the World Bank and the International Monetary Fund [IMF] estimated the global amount of regular ATMs per 100,000 adults in 2017 to be 43.504 (The World Bank & International Monetary Fund, 2017). The corresponding global population of 2017 was 7.53 billion people (United Nations Population Division, 2017) of which 8.696% were aged 65 years and above (The World Bank, 2017a), and 65.363% were aged between 15 and 64 years (The World Bank, 2017b). Together 74.059% of the global population, about 5,576,642,700 people, were above 15 years old in 2017. This places the global amount of ATMs at roughly 2,426,063 based on the IMF, World Bank and United Nation statistics. The ATM Industry Association [ATMIA] as *“leading non-profit trade association representing the entire global ATM industry”* (ATM Industry Association, 2019a) estimates the amount of installed ATMs at *“over 2.2 million”* (ATM Industry Association, 2019b) machines globally.

Contrasting the amount of cryptoasset capable ATMs with the amount of regular ATMs (4628 machines to ~2.4 million machines) reveals the prevalence of Bitcoin technology still to be in its infancy. With consideration to the fact that Bitcoin is still the most popular distributed ledger technology, the challenges in instrument of payment, security and regulation clarify that much is still to be done before the technology will be widely adopted.

4.2.3 Environmental impact of Bitcoin

Bitcoin's proof of work consensus mechanism requires network nodes to provide computing resources to participate in its activity in exchange for receiving Bitcoin currency. Since 2017 the technology platform has received more and more media as well as public attention due to rising Bitcoin valuation (Figure 37).

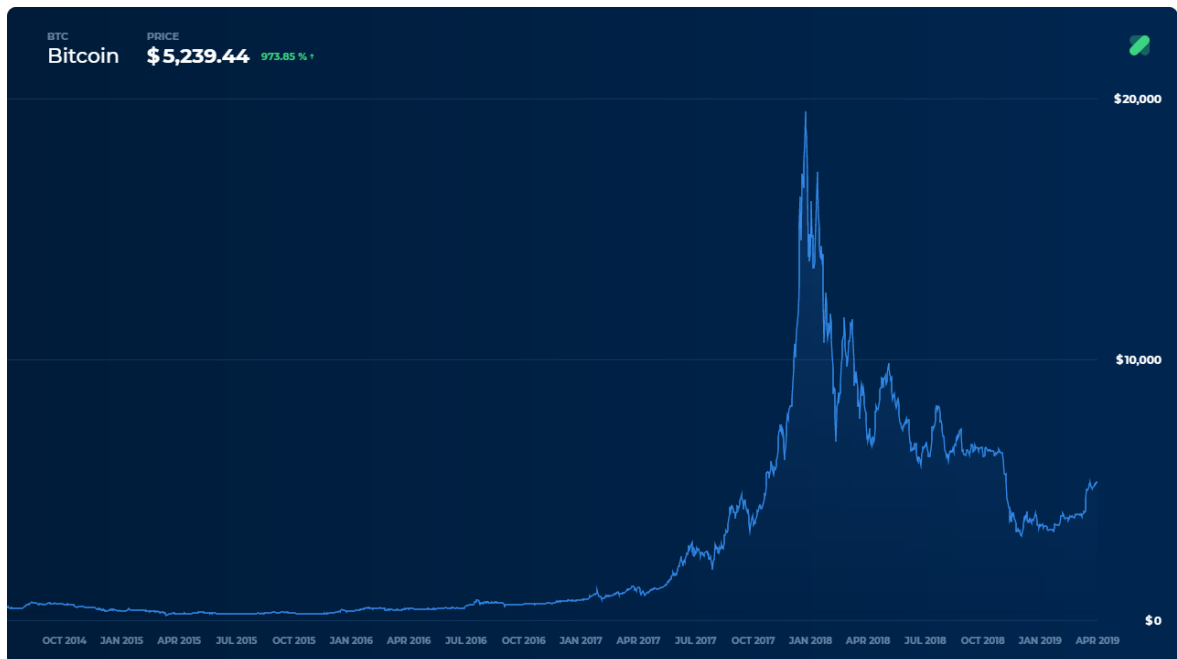


Figure 37: Bitcoin currency exchange price (USD) development 2014 to 2019 (Coinranking, 2019b)

This led to an increase in participants joining the network and a “*hardware arms race*” (O'Dwyer & Malone, 2014, p. 282) in order to increase the likelihood of being the node that mines a new Block for the network and gains the currency reward. The Bitcoin platform is averaged in such a way, that the algorithm expects the discovery of a new Block at around ten minutes. The method to keep it this way is the difficulty of solving the mathematical puzzle under the PoW scheme. With the increase in processing power provided to the network the solutions require a more and more calculating intense process in order to keep the Block discovery time average at ten minutes.

This has driven the overall network energy consumption to an estimated 56.093 terawatt hours [TWh] per year on the 19th of April 2019 (Digiconomist, 2019a) for the Bitcoin network (Figure 38).

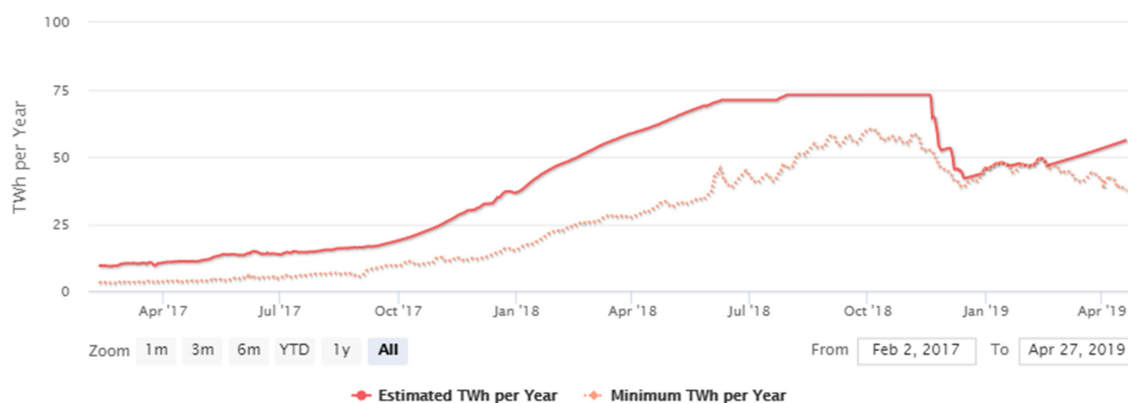


Figure 38: Bitcoin energy consumption (Digiconomist, 2019a)

The total energy consumption for Switzerland, Greece and Colombia in comparison are 58.45 TWh (2015 estimate), 53.05 TWh (2015 estimate) and 60.11 TWh (2017 estimate) respectively (Central Intelligence Agency, 2019). According to the CIA World Factbook estimates (ibid.), the Bitcoin network consumes more energy than 170 individual countries on planet earth.

Adding five other major distributed ledger platforms (Bitcoin Cash, Ethereum, Litecoin, Monero and ZCash) to the Bitcoin energy consumption index reveals the following Figure 39.

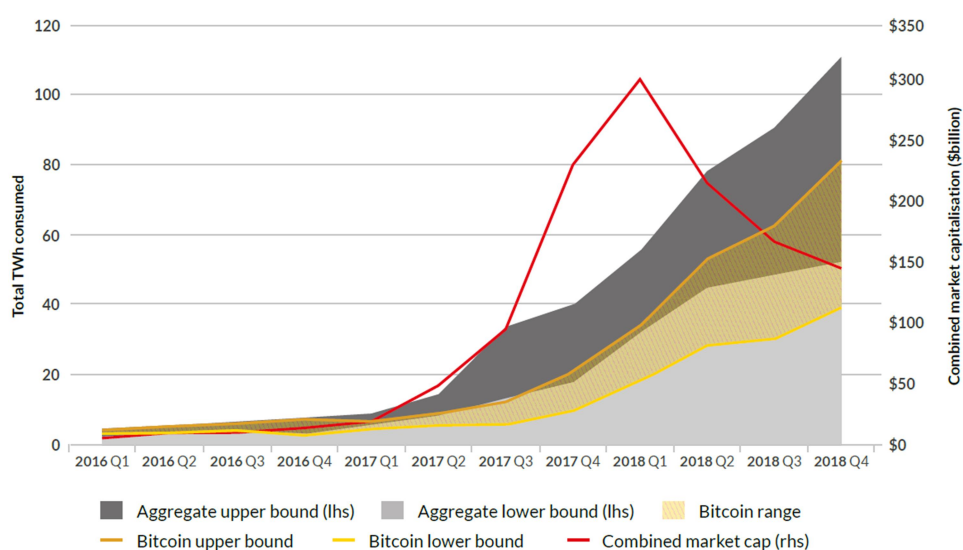


Figure 39: Estimated energy consumption range for six major DLTs (Rauchs, et al., 2018, p. 82)

The combined energy consumption of these six platforms was estimated to be 111 terawatt hours annually (Rauchs, et al., 2018). This is five TWh annually more than the estimated total annual energy consumption of the Netherlands in 2015, as well as more energy consumption than 183 individual countries (Central Intelligence Agency, 2019).

4.2.4 Bitcoin Volatility

Figure 37 indicates a sharp rise and fall of Bitcoins currency valuation in USD between November 2017 and April 2018 from USD 6,235 up to USD 19,500 down again to USD 7,034 (Coinranking, 2019b) with a current valuation of USD 5,270 (20. April 2019). It poses the question about the reliability and volatility of the Bitcoin as a currency. Baur, et al. argue *“Bitcoin’s return properties are very different from traditional asset classes including currencies”* (2018, p. 187) and find that *“Bitcoin is mainly used as a speculative investment despite or due to its high volatility and large returns”* (ibid. p. 178). This notion is supported by Cheah & Fry (2015) attributing Bitcoin a fundamental value of zero due to its high volatility and thus being prone to speculative bubbles. Some research also indicates intentional manipulation of Bitcoin valuation through bots (Gandal, et al., 2018) or Ponzi scheme like pump-and-dump scams (Simser, 2015) (Hamrick, et al., 2018). It remains questionable if the observed volatility in the past can be overcome on a not-access restricted distributed ledger technology under which users are only restricted by the amount of physical processing power they are able to supply to the network.

4.3 Conclusion

This chapter discussed distributed ledger technology adoption based on the example of Satoshi Nakamoto’s Bitcoin.

- Despite its almost eleven year old tenure as the first viable distributed ledger technology and its inspiration of countless other technology platforms seeking to improve upon technological shortcomings (such as the proof of work consensus mechanism), Bitcoin has only gained popularity as speculative financial instrument. Only few business transactions can be conducted using its currency form, since accepting businesses, as well as teller machines for fiat currency conversion are few and far between on a global scale.
- The estimated energy consumption of the network is massive and rivals that of Switzerland.

- Additionally, the technology has been proven to be unreliable from a security perspective in two major thefts.

Based on these shortcomings and the lack of code based smart contract implementation on Bitcoin, it appears unlikely for it to become a widely adopted technology platform outside speculative investment. The Ethereum platform on the other hand was iterated and built with improving upon Bitcoin's shortcomings in mind and allows for Turing-complete programming logic to facilitate autonomous smart contracts (Buterin, 2014). It already outperforms Bitcoin in some metrics (Figure 35) and as part of Blockchain 3.0 (Swan, 2015) is more likely to be widely adopted in the future than its parent Bitcoin.

Chapter 5 – Summary

Satoshi Nakamoto released the Bitcoin technology platform with the following message included in Bitcoin's genesis Block³¹: "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*" (De Filippi & Wright, 2018, p. 205). The message most likely refers to The Times article "*Chancellor Alistair Darling on brink of second bailout for banks*" (Elliott & Duncan, 2009) published at 12:00 am on the 3rd of January 2009. Speculating on the meaning of this message is difficult without knowledge of the identity of Nakamoto. It is possible though, that the publication of Bitcoin including this specific message was done, because the authoring entity wished to provide the means to combat banking and financial system failure in the future. However this is also speculation, the real reason might never be known outside Nakamoto.

Nevertheless, it served as inspiration for this thesis, which explored two research questions:

1. Has information mismanagement contributed to banking failure during the global financial crisis from 2008 to 2012?
2. Can distributed ledger technology address this information handling negligence and provide a solution to minimize the risk of future large scale bank failures?

In order to do so, chapter 2 analysed and quantified banking failures in the United States and in Europe. During the investigation, examples of all four types of information failure (Figure 1) are found in the proceedings of the aftermath of the global financial crisis 2008 to 2012. These information management malpractices contributed to bank failures and some, such as information secrecy, are still commonly employed in the industry.

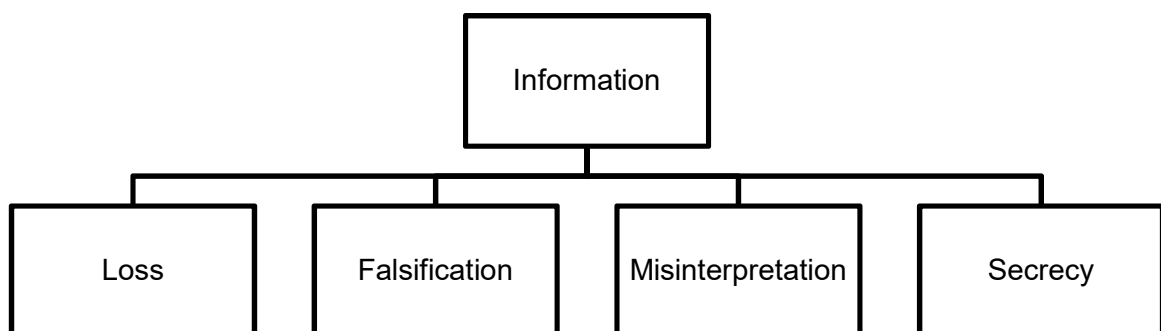


Figure 1: Four types of information failure

³¹ This Medium post explains the decryption process how to access the message: <https://medium.com/splytcore/simple-decryption-of-satoshi-nakamotos-hidden-message-in-the-blockchain-42b5fe9b3c72> [accessed: 28th of December 2018].

In chapter 3, this thesis proposes and discusses distributed ledger technology as an alternative to current data management solutions in order to resolve the problem of information mismanagement and improve upon the regulatory processes around banking auditing. A public, permissionless distributed ledger, for example through Blockchain technology and smart contracts, would allow moving from the current auditing process (Figure 5) prone to information carelessness to a system (Figure 6) allowing for full information and transaction access for all interested parties.

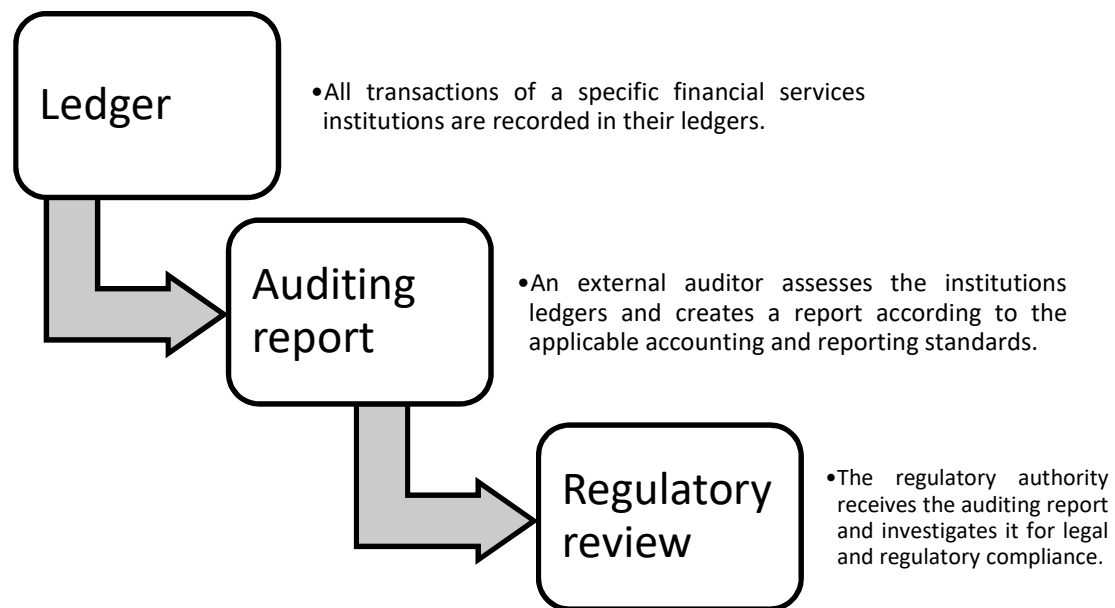


Figure 5: Current, simplified auditing process chart

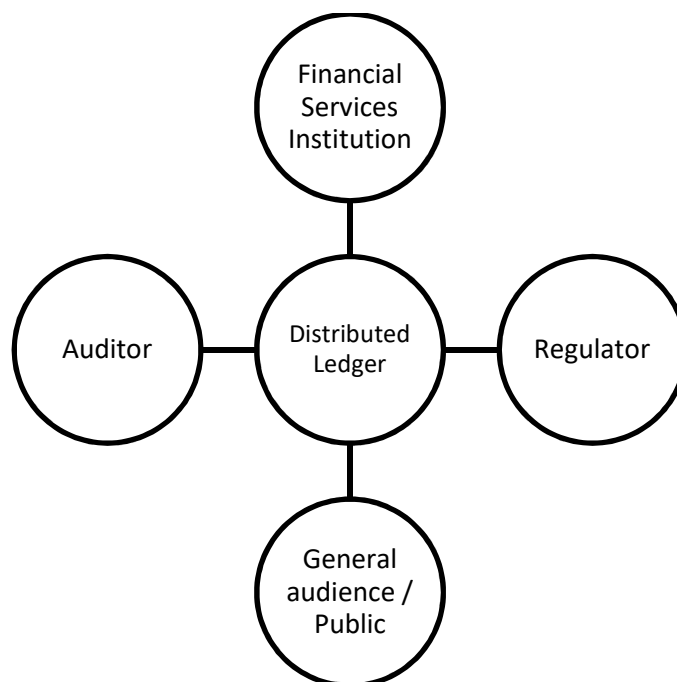


Figure 6: Simplified auditing process chart for distributed ledger

Chapter four contrasts the Bitcoin technology and currency with fiat currency and finds limitations in conducting business through the platform, as well as identifies energy consumption as a problem for distributed ledger technologies.

With regards to the two research questions, the answer to both must be “Yes”. Distributed ledger technology can provide a potential technological solution to information mismanagement caused banking failure by opening up the information and transaction pool of financial services institutions to provide full transparency at any given time.

Due to constraints in the technology itself (e.g. security, network speed for large ledgers, etc.), owed to the young nature of the different versions of DLT 1.0, 2.0 and 3.0 (Swan, 2015), it is unlikely, that a decentralized permissionless Blockchain will be employed for the purposes discussed in this thesis in the next five to ten years. Nonetheless, once the technology is matured and the basic parameters of regulatory frameworks are set, it will provide an effective tool to minimize the risk of banking failures. Financial services institutions at that point, will become autonomously managed decentralized organisations that are automatically supervised by every member wishing to do so.

5.1 Lessons Learned

5.1.1 Distributed Ledger Technology – a Two Edged Sword

The global industry analyst Gartner marks Blockchain technology to be five to ten years away from mainstream adoption (*“Plateau of Productivity”*) and at the end of hype scenario (*“Peak of Inflated Expectations”*) garnering large popular attention (Figure 40).

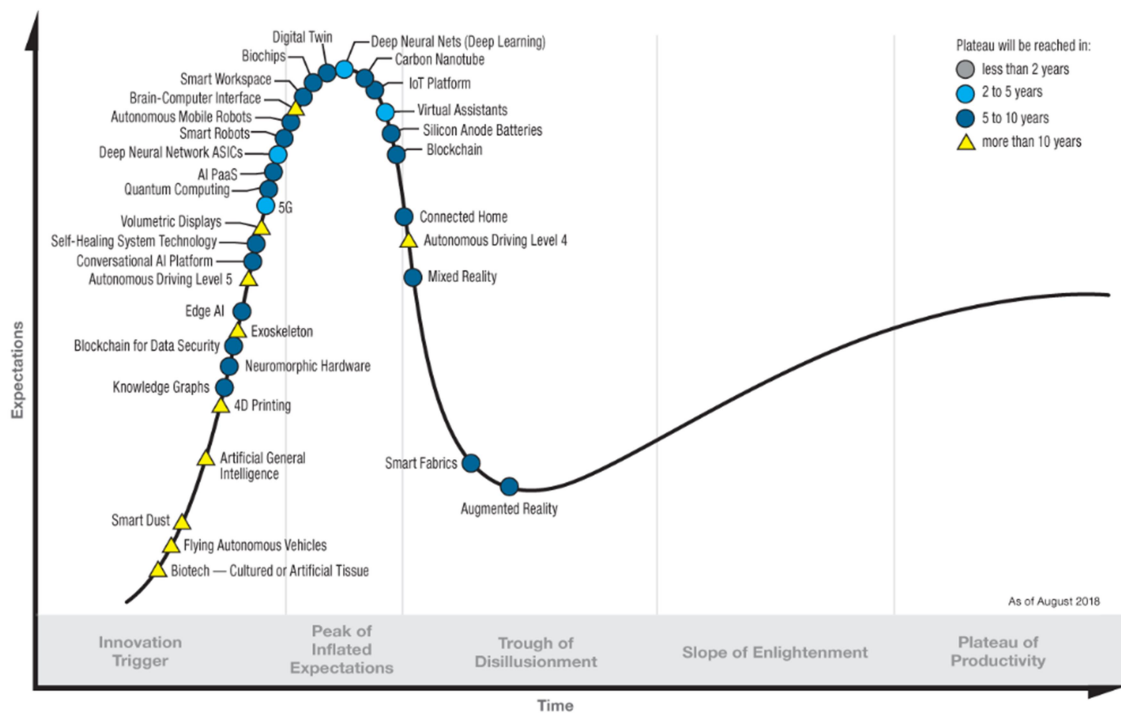


Figure 40: Hype Cycle for Emerging Technologies, 2018 (Panetta, 2018)

This popular attention was found in particular during the period November 2017 to April 2018 when Bitcoin currency speculations drove the valuation close to USD 20,000. The speculative nature of these investments, the hope of many investors (without full understanding of the risks of the new technology) to have found a get rich quick scheme (Vasek & Moore, 2015) and the accompanying media coverage support Gartner's notion, that there is still work to be done until distributed ledger technology and Blockchain are widely adopted. This strong interest is also mirrored in research where Konstantinidis et al. (2018) found a drastic increase of primary studies published from 2015 to 2017 (Figure 41).

Annual distribution of our primary studies

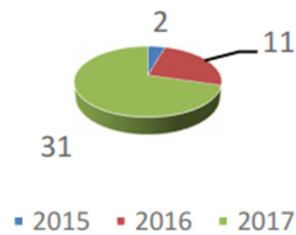


Figure 41: Primary Blockchain studies distribution per year (Konstantinidis, et al., 2018, p. 392)

In this context, the media attention might even have negative impacts on the rate of adoption, since the speculative bubble, as well as technology exploit based thefts have created a bad reputation for Blockchain technologies. It should be clear that based on individual use cases, a specific technology, fitting for the required scenarios, should be chosen instead of propagating a one fits all solution. This is true for existing technologies and does also apply to distributed ledgers. They are not the right choice under every circumstance some have made them out to be. To provide some guidance, Figure 42 below provides a flowchart to identify specific use cases under which Blockchain would be helpful.

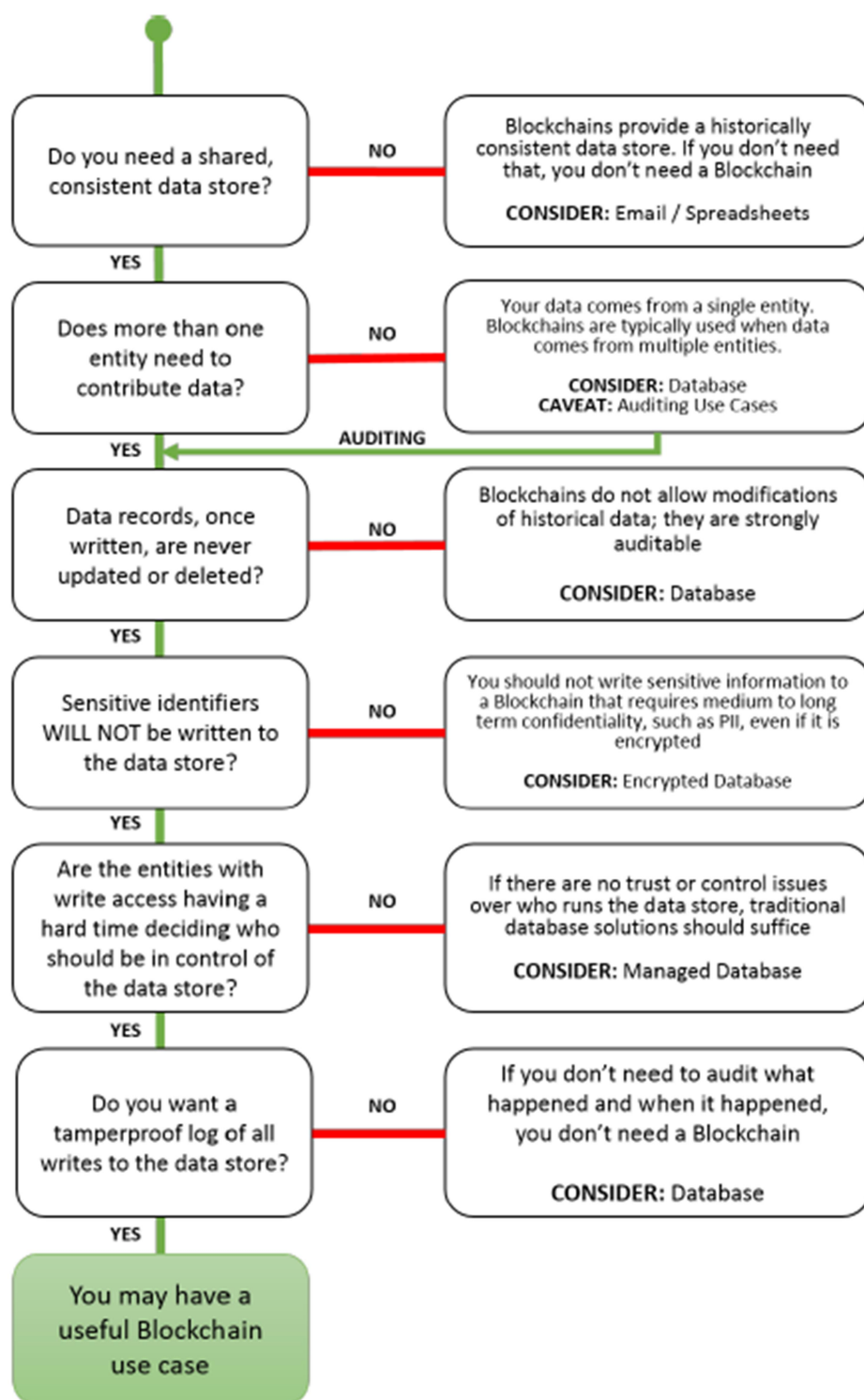


Figure 42: Flowchart to identify Blockchain use cases (Yaga, et al., 2018, p. 42)

5.1.2 Data on Failed Banks in Europe

Contrary to the United States of America where the FDIC publishes annual data on bank failure among their member institutions, the situation in Europe is quite different. On level of the European Union, no similarly tasked organization exists, as banking insurance is coordinated on a national level with the individual associations only having a common communication platform through the EFDI. As a result, published information on the scale of the FDIC is scarce within Europe, as no obligation for the individual deposit insurer exists to provide their data to the public. This prevents an effective analysis of the full extent of banking failure in Europe.

5.1.3 The Unclear Legal Situation of Distributed Ledger Technology

Satoshi Nakamoto paved the way for a new technology platform based on a synthesis of fast peer-to-peer global networking, advanced cryptography and data resilience. It brought with it a virtual currency, not backed through a precious metal (Eichengreen, 1995), commodity standard (Hall, 1982) or governments and the assets of a national central bank, for example the Federal Reserve Banks [Feds] in the United States (Board of Governors of the Federal Reserve System, 2017). As a result of Nakamoto's proposals, enthusiasts, cryptographers, early adopters and companies have taken it upon themselves to build and improve upon DLT systems, but the aligned currencies still fall into a class of unregulated activities and unclear legal status. The European Central Bank [ECB] warned: "*Currently, if VCS [Virtual Currency Schemes] have a legal status at all, it is unclear and the key actors are generally neither regulated nor supervised*" (European Central Bank, 2015). Nonetheless, the European Court of Justice considered Bitcoin to be a means of payment (European Court of Justice, 2015) but specifically referred to the virtual currency and did not make a statement on the technology platform itself. Concerns about the privacy of public, permissionless distributed ledgers (Gabison, 2016) as well as the legal validity of self-executing and –enforcing smart contracts (Wright & De Filippi, 2015) have given rise to the discussion of *Lex Cryptographia* (De Filippi & Wright, 2018). Based on the idea of *Lex Informatica* (Reidenberg, 1997) *Lex Cryptographia* is considered to be a new, yet fully to be defined, subset of laws and regulations influenced by four regulatory levers (code, law, market forces and social norms) (De Filippi & Wright, 2018) that would remove trusted intermediaries completely, but rather re-define their roles to play.

5.2 Conclusion

Considering that DLTs are still in their early phases (Figure 40) of implementation and adoption it is not surprising that regulatory frameworks are still underdeveloped and discussed by legal decision makers. Federal discussion platforms, such as the EU Blockchain Observatory and Forum³² provide the opportunity to contribute and participate in the development of regulatory standards for the future of the technology.

With the words of Bob Dylan: “*The Times They Are a-Changin*” (1963) and given time, as well as solutions to such problems as security, environmental impact and networking speed, distributed ledger technology might prove as useful as the internet. It is important to keep in mind though, it is not a one-fit-all solution to solve every problem it sometimes is made out to be.

³² <https://www.eublockchainforum.eu/>

Works Cited

- Alper, C. E., 1933. Banking Act of 1933 (Glass-Steagall Bill). *St. John's Law Review*, 8(1), pp. 193-196.
- Androulaki, E. et al., 2018. *Hyperledger fabric: a distributed operating system for permissioned blockchains*. Porto, ACM.
- ATM Industry Association, 2019a. *ABOUT ATMIA*. [Online]
Available at: <https://www.atmia.com/about-us/overview/mission-statement--profile/>
[Accessed 09th February 2019].
- ATM Industry Association, 2019b. *ATM Industry Association*. [Online]
Available at: <https://www.atmia.com/showrooms/atm-industry-association/1101/>
[Accessed 09th February 2019].
- Ayed, A. B., 2017. A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications (IJNSA)*, 9(3), pp. 1-9.
- Barborak, M., Dahbura, A. & Malek, M., 1993. The consensus problem in fault-tolerant computing. *ACM Computing Surveys (CSUR)*, 25(2), pp. 171-220.
- Bastiaan, M., 2015. *Preventing the 51%-Attack: a Stochastic Analysis of Two Phase Proof of Work in Bitcoin*. [Online]
Available at:
<https://pdfs.semanticscholar.org/0336/6d1fda3b24651c71ec6ce21bb88f34872e40.pdf>
[Accessed 3rd January 2019].
- Baur, D. G., Hong, K. & Lee, A. D., 2018. Bitcoin: Medium of exchange or speculative assets?. *Journal of International Financial Markets, Institutions & Money*, Volume 54, pp. 177-189.
- Becker, J. et al., 2013. Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency. In: R. Böhme, ed. *The Economics of Information Security and Privacy*. Heidelberg: Springer, pp. 135-156.
- Bentov, I., Lee, C., Mizrahi, A. & Rosenfeld, M., 2014. *Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake*, s.l.: International Association for Cryptologic Research.
- Berger, A. N., Kashyap, A. K. & Scalise, J. M., 1995. The Transformation of the U.S. Banking Industry: What a Long, Strange Trip It's Been. *Brookings papers on economic activity*, Issue 2, pp. 55-218.

Bhattacharya, S. & Nyborg, K. G., 2013. Bank Bailout Menus. *The Review of Corporate Finance Studies*, 2(1), pp. 29-61.

Bisaschi, A., 2003. The accounting system of the Venerable Society of the Living and the Dead of Parma in medieval times. *Accounting History*, 8(1), pp. 89-111.

Board of Governors of the Federal Reserve System, 2017. *Federal Reserve Act - Section 16. Note Issues*. [Online]

Available at: <https://www.federalreserve.gov/aboutthefed/section16.htm>

[Accessed 24 February 2019].

Brenna, G., Poppensieker, T. & Schneider, S., 2009. *Understanding the bad bank*.

[Online]

Available at: <https://www.mckinsey.com/industries/financial-services/our-insights/understanding-the-bad-bank>

[Accessed 17 March 2019].

Bryer, R. A., 1993. Double-Entry Bookkeeping and the Birth of Capitalism: Accounting for the Commercial Revolution in Medieval Northern Italy. *Critical Perspectives on Accounting*, 4(2), pp. 113-140.

Bulow, J. I. & Shoven, J. B., 1978. The bankruptcy decision. *The Bell Journal of Economics*, 9(2), pp. 437-456.

Burkhardt, D., Werling, M. & Lasi, H., 2018. *Distributed Ledger - 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*. Stuttgart, IEEE.

Buterin, V., 2014. *Ethereum White Paper: A next-generation smart contract and decentralized application platform*. [Online]

Available at:

<https://pdfs.semanticscholar.org/0dbb/8a54ca5066b82fa086bbf5db4c54b947719a.pdf>

[Accessed 28 December 2018].

Butler, S., 1863. *Darwin among the machines - [To the editor of the press, Christchurch, New Zealand, 13 June, 1863]*. [Online]

Available at: <http://nzetc.victoria.ac.nz/tm/scholarly/tei-ButFir-t1-g1-t1-g1-t4-body.html>

[Accessed 12 January 2019].

Camebridge Business English Dictionary, 2019. *bad bank*. [Online]

Available at: <https://dictionary.cambridge.org/dictionary/english/bad-bank>

[Accessed 20 April 2019].

Caplan, D. H., Dutta, S. K. & Marcinko, D. J., 2012. Lehman on the Brink of Bankruptcy: A case about Agressive Application of Accounting Standards. *Issues in Accounting Education*, 27(2), pp. 441-459.

Carruthers, B. G. & Nelson Espeland, W., 1991. Accounting for Rationality: Double-Entry Bookkeeping and the Rhetoric of Economic Rationality. *The American Journal of Sociology*, 97(1), pp. 31-69.

Carswell, S., 2018a. *David Drumm guilty verdict – all you need to know in two minutes*. [Online]

Available at: <https://www.irishtimes.com/news/crime-and-law/courts/circuit-court/david-drumm-guilty-verdict-all-you-need-to-know-in-two-minutes-1.3521436>

[Accessed 10 February 2019].

Carswell, S., 2018b. *David Drumm jailed for six years for conspiracy to defraud*. [Online]

Available at: <https://www.irishtimes.com/news/ireland/irish-news/david-drumm-jailed-for-six-years-for-conspiracy-to-defraud-1.3537143>

[Accessed 10 February 2019].

Cebula, R. J., Koch, J. V. & Fenili, R. N., 2011. The Bank Failure Rate, Economic Conditions and Banking Statutes in the U.S., 1970–2009. *Atlantic Economic Journal*, 39(1), pp. 39-46.

Central Intelligence Agency, 2019. *The World Factbook*. [Online]

Available at: <https://www.cia.gov/library/publications/the-world-factbook/rankorder/2233rank.html>

[Accessed 10th February 2019].

Chaboud, A., Chiquoine, B., Hjalmarsson, E. & Vega, C., 2014. Rise of the machines: Algorithmic trading in the foreign exchange market. *The Journal of Finance*, 69(5), pp. 2045-2084.

Chalaemwongwan, N. & Kurutach, W., 2018. *State of the art and challenges facing consensus protocols on blockchain*. Chiang Mai, IEEE.

Chaum, D., 1983. Blind Signatures for Untraceable Payments. In: D. Chaum, R. L. Rivest & A. T. Sherman, eds. *Advances in Cryptology*. Boston: Springer.

Chaum, D., Fiat, A. & Naor, M., 1988. *Untraceable Electronic Cash*. New York, Springer.

Cheah, E.-T. & Fry, J., 2015. Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. *Economics Letters*, Volume 130, pp. 32-36.

Christidis, K. & Devetsikiotis, M., 2016. Blockchains and smart contracts for the internet of things. *Ieee Access*, Volume 4, pp. 2292-2303.

Claessens, S. & Kodres, L., 2014. *The regulatory responses to the Global Financial Crisis: Some uncomfortable questions*, s.l.: International Monetary Fund.

Coin ATM Radar, 2019a. *Coin ATM Radar*. [Online]

Available at: <https://coinatmradar.com/>

[Accessed 20 April 2019].

Coin ATM Radar, 2019b. *Crypto ATM Number Net Changes*. [Online]

Available at: <https://coinatmradar.com/charts/net-growth/>

[Accessed 20 April 2019].

Coin ATM Radar, 2019c. *Crypto ATM Distribution by Continents and Countries*. [Online]

Available at: <https://coinatmradar.com/charts/geo-distribution/>

[Accessed 20 April 2019].

Coinbase, 2019. *Coinbase*. [Online]

Available at: <https://www.coinbase.com/price>

[Accessed 20 April 2019].

Coinmap, 2019. *coinmap.org*. [Online]

Available at: <https://coinmap.org/#/world/11.26461221/20.39062500/3>

[Accessed 16th April 2019].

CoinMarketCap, 2019. *CoinMarketCap*. [Online]

Available at: <https://coinmarketcap.com/>

[Accessed 20 April 2019].

Coinranking, 2019a. *Coinranking*. [Online]

Available at: <https://coinranking.com/>

[Accessed 20 April 2019].

Coinranking, 2019b. *Bitcoin Price*. [Online]

Available at: <https://coinranking.com/coin/bitcoin-btc>

[Accessed 20 April 2019].

Congress United States of America, 1933. *Banking Act of 1933*. Washingto D.C.:

Congress United States of America.

Conoscenti, M., Vetrò, A. & De Martin, J. C., 2016. *Blockchain for the Internet of Things: A systematic literature review*. Agadir, IEEE.

Curry, T. & Shibut, L., 2000. The Cost of the Savings and Loan Crisis: Truth and Consequences. *FDIC Banking Review*, 13(26), pp. 26-35.

Daly, P., 2011. *Statement issued in accordance with Bye-Law 19.8 of the Disciplinary Bye-Laws of Chartered Accountants*. [Online]

Available at: <http://www.carb.ie/documents/Statement%20issued%20by%20CARB%2014-Sep-11.pdf>

[Accessed 24th March 2019].

DB-Engines, 2019. *DB-Engines Complete Ranking*. [Online]

Available at: <https://db-engines.com/en/ranking>

[Accessed 06 April 2019].

De Angelis, S. et al., 2018. *PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain*. Milan, Italian Conference on Cyber Security.

De Filippi, P. & Wright, A., 2018. *Blockchain and the Law*. 1st ed. Cambridge: Harvard University Press.

de la Rosa, J. L. et al., 2016. *On Intellectual Property in Online Open Innovation for SME by means of Blockchain and Smart Contracts*. Barcelona, Proceedings of the 3rd Annual World Open Innovation Conference WOIC.

Demyanyk, Y. & Van Hemert, O., 2009. Understanding the subprime mortgage crisis. *The Review of Financial Studies*, 24(6), pp. 1848-1880.

Die Berater der Reichen und Mächtigen - Die Macht der "Big Four". 2019. [Film] Directed by Michael Wech, Petra Nagel, Massimo Bognanni, Petra Blum, Georg Wellmann, Lena Kampf, Katja Riedel. Germany: WDR Doku.

Digiconomist, 2019a. *Bitcoin Energy Consumption Index*. [Online]

Available at: <https://digiconomist.net/bitcoin-energy-consumption>

[Accessed 19 April 2019].

Dinh, T. T. A. et al., 2018. Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering*, 30(7), pp. 1366-1385.

Dylan, B., 1963. *The Times They Are a-Changin'*. [Sound Recording] (Columbia Studios).

Eichengreen, B., 1995. *Golden Fetters: The Gold Standard and the Great Depression, 1919-1939*. 1st ed. Oxford: Oxford University Press.

Elejalde-Ruiz, A., 2015. *\$13M penalty for background check errors that cost jobs, hurt reputations - Chicago Tribune*. [Online]

Available at:

<https://webcache.googleusercontent.com/search?q=cache:LzrlhXxiRIYJ:https://www.chicagotribune.com/business/ct-background-check-penalties-1030-biz-20151029-story.html+&cd=1&hl=en&ct=clnk&gl=ie>

[Accessed 16 March 2019].

Elliott, F. & Duncan, G., 2009. *The Times - Chancellor Alistair Darling on brink of second bailout for banks*. [Online]

Available at: <https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h>

[Accessed 23rd November 2018].

Engen, D. T., 2018. *The Economy of Ancient Greece (eh.net)*. [Online]

Available at: <https://eh.net/encyclopedia/the-economy-of-ancient-greece/>

[Accessed 26 December 2018].

European Central Bank, 2015. *Virtual currency schemes - a further analysis*, Frankfurt am Main: European Central Bank.

European Court of Justice, 2015. *Skatteverket (Swedish tax authority) v. David Hedqvist (C-264/14)*. [Online]

Available at:

<http://curia.europa.eu/juris/document/document.jsf?jsessionid=5CDBC6759C478208FDB085FC8560861B?text=&docid=170305&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4079936>

[Accessed 10th March 2019].

European Parliament, 2013. Directive 2013/11/EU on alternative dispute resolution for consumer disputes and amending Regulation. *Official Journal of the European Union*, 165(63), pp. 1-17.

Eyal, I., 2017. Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities. *Computer*, 50(9), pp. 38-49.

Eyal, I., Gencer, A. E., Sirer, E. G. & Renesse, R. v., 2016. *Bitcoin-NG: A Scalable Blockchain Protocol*. Santa Clara, Usenix - The advanced computing systems association.

FDIC, 2017. *Who is the FDIC?*. [Online]

Available at: <https://www.fdic.gov/about/learn/symbol/>

[Accessed 09 February 2019].

Ferreira Jesus, E., Chicarino, V. R., de Albuquerque, C. V. N. & de A. Rocha, A. A., 2018. A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack. *Security and Communication Networks*, Volume 2018, p. 27.

Froystad, P. & Holm, J., 2015. *Blockchain: Powering the internet of value - Whitepaper*. [Online]

Available at: <https://www.evry.com/globalassets/insight/bank2020/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf>

[Accessed 18 February 2019].

Gabison, G., 2016. Policy Considerations for the Blockchain Technology Public and Private Applications. *Science and Technology Law Review*, 19(3), pp. 327-350.

Gandal, N., Hamrick, J., Moore, T. & Oberman, T., 2018. Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics*, Volume 95, pp. 86-96.

GAO, 2013. *Report to Congressional Requesters - Financial Regulatory Reform - Financial Crisis Losses and Potential Impacts of the Dodd-Frank Act*, Washington D.C.: United States Government Accountability Officeus .

Gatteschi, V. et al., 2018. Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?. *Future Internet*, 10(2), p. 16.

Gervais, A. et al., 2016. *On the security and performance of proof of work Blockchains*. Vienna, ACM.

Gleeson-White, J., 2011. *Double Entry: How the merchants of Venice shaped the modern world - and how their invention could make or break the planet*. 1st ed. Sydney: Allen & Unwin.

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

Hall, R. E., 1982. Explorations in the Gold Standard and Related Policies. In: R. E. Hall, ed. *Inflation: Causes and Effects*. Chicago: University of Chicago Press, pp. 111-122.

Hamrick, J. et al., 2018. The Economics of Cryptocurrency Pump and Dump Schemes. *SSRN*, p. 19.

Hannaford-Agor, P. L., 2013. *Measuring the Cost of Litigation: Findings from a survey of trial lawyers*, Williamsburg: NCSC - National Center for State Courts.

Hardin, G., 1968. The Tragedy of the Commons. *Science*, 162(3859), pp. 1243-1248.

Hennessy, C. A., 2004. Tobin's Q, Debt Overhang, and Investment. *The Journal of Finance*, 59(4), pp. 1717-1742.

Hines, C., Kreuze, J. & Langsam, S., 2011. An analysis of Lehman Brothers bankruptcy and Repo 105 transactions. *American Journal of Business*, 26(1), pp. 40-49.

Hoggson, N. F., 1926. *Banking Through The Ages*. 1st ed. New York: Dodd, Mead & Company.

House of the Oireachtas, 2016. *Report of the Joint Committee of Inquiry into the Banking Crisis*, Dublin: House of the Oireachtas.

Houy, N., 2016. The Bitcoin Mining Game. *Ledger*, Volume 1, pp. 53-68.

IBRC - Irish Bank Resolution Corporation, 2018. *Irish Bank Resolution Corporation Limited (in Special Liquidation) ("IBRC")*. [Online]
Available at: <http://www.ibrc.ie/>
[Accessed 27 January 2019].

Jeffers, A. E., 2011. How Lehman Brothers used Repo 105 to manipulate their financial statements. *Journal of Leadership, Accountability and Ethics*, 8(5), pp. 44-55.

Jensen, M. C. & Meckling, W. H., 1976. Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), pp. 305-360.

Jones, K. D. & Critchfield, T., 2005. Consolidation in the U.S. Banking Industry: Is the "Long, Strange Trip" About to End?. *FDIC Banking Review*, 17(4), pp. 31-61.

Joshi, A. P., Han, M. & Wang, Y., 2018. A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing*, 1(2), pp. 121-147.

Karame, G., Androulaki, E. & Capkun, S., 2012. *Double-spending fast payments in bitcoin*. Raleigh, ACM.

Ketz, J. E., 2003. *Hidden Financial Risk - Understanding Off-Balance Sheet Accounting*. 1st ed. Hoboken: John Wiley & Sons, Inc..

Kiayias, A., Russell, A., David, B. & Oliynykov, R., 2017. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. In: J. Katz & H. Shacham, eds. *Advances in Cryptology – CRYPTO 2017*. Santa Barbara: Springer, pp. 357-388.

Kim, J. J., 2017. *Contract*. [Online]
Available at: <https://www.law.cornell.edu/wex/contract>
[Accessed 06 April 2019].

King, S. & Nadal, S., 2012. *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. [Online]

Available at: <https://peercoin.net/whitepapers/peercoin-paper.pdf>

[Accessed 2 February 2019].

King, T. A., 2006. *More than a numbers game: a brief history of accounting*. 1st ed. Hoboken: John Wiley & Sons, Inc..

Kishigami, J. et al., 2015. The Blockchain-Based Digital Content Distribution System. In: *Proceedings of IEEE Fifth International Conference on Big Data and Cloud Computing*. 2015: IEEE, pp. 187-190.

Kölvart, M., Poola, M. & Rull, A., 2016. Smart Contracts. In: T. Kerikmäe & A. Rull, eds. *The Future of Law and eTechnologies*. Heidelberg: Springer International Publishing, pp. 133-147.

Konstantinidis, I. et al., 2018. Blockchain for Business Applications: A Systematic Literature Review. In: W. Abramowicz & A. Paschke, eds. *Business Information Systems - 21st International Conference, BIS 2018, Berlin, Germany, July 18-20, 2018, Proceedings*. Berlin: Springer, pp. 384-399.

Kroll, J. A., Davey, I. C. & Felten, E. W., 2013. *The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries*. Georgetown, Workshop on the Economics of Information Security (WEIS).

Lamport, L., Shostak, R. & Pease, M., 1982. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, 4(3), pp. 382-401.

Lee Kuo Chuen, D., 2015. *Handbook of digital currency*. 1st ed. London: Elsevier.

Legal Information Institute, 2019a. *Consideration*. [Online]

Available at: <https://www.law.cornell.edu/wex/consideration>

[Accessed 06 April 2019].

Legal Information Institute, 2019b. *Capacity*. [Online]

Available at: <https://www.law.cornell.edu/wex/capacity>

[Accessed 06 April 2019].

Lehdonvirta, V. & Castronova, E., 2014. *Virtual economies: Design and analysis*. 1st ed. Cambridge: MIT Press.

Levin, A. L. & Colliers, D. D., 1985. Containing the Cost of Litigation. *Rutgers Law Review*, 37(2), pp. 219-252.

Lewis, M., 2010. *The Big Short: Inside the Doomsday Machine*. 1st ed. New York: W. W. Norton & Company.

Li, P., Wang, G., Chen, X. & Xu, W., 2018. *Gosig: Scalable Byzantine Consensus on Adversarial Wide Area Network for Blockchains*. [Online]

Available at: <https://arxiv.org/abs/1802.01315>

[Accessed 20 February 2019].

Li, X. et al., 2017. A Survey on the Security of Blockchain Systems. *Future Generation Computer Systems*, pp. 1-25.

Luu, L. et al., 2016. *Making Smart Contracts Smarter*. Vienna, ACM.

Malkhi, D. & Reiter, M., 1998. Byzantine quorum systems. *Distributed computing*, 11(4), pp. 203-213.

Martinelli, A., 1974. *The Origination and Evolution of Double Entry Bookkeeping to 1440 (PhD Thesis)*. Denton: North Texas State University.

Maull, R. et al., 2017. Distributed ledger technology: Applications and implications. *Strategic Change*, 26(5), pp. 481-489.

McCorry, P., Shahandashti, S. F. & Hao, F., 2017. A Smart Contract for Boardroom Voting with Maximum Voter Privacy. In: A. Kiayias, ed. *21st International Conference on Financial Cryptography and Data Security*. Sliema: Springer, pp. 357-375.

McMillian, R., 2014. *THE INSIDE STORY OF MT. GOX, BITCOIN'S \$460 MILLION DISASTER*. [Online]

Available at: <https://www.wired.com/2014/03/bitcoin-exchange/>

[Accessed 11th November 2018].

Merriam-Webster, 2018. *Merriam-Webster*. [Online]

Available at: <https://www.merriam-webster.com/dictionary/ledger>

[Accessed 29 December 2018].

Morabito, V., 2017. *Business Innovation Through Blockchain*. 1st ed. Milan: Springer International Publishing.

MySQL Documentation Team, 2019. *MySQL Documentation*. [Online]

Available at: <https://dev.mysql.com/doc/>

[Accessed 06 April 2019].

Nakamoto, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. s.l.:s.n.

Natoli, C. & Gramoli, V., 2016. *The Blockchain Anomaly*. Cambridge, IEEE.

O'Dwyer, K. J. & Malone, D., 2014. *Bitcoin Mining and its Energy Footprint*. Limerick, ISSC 2014/CIICT 2014.

Oliver, J., 2016. *Credit Reports: Last Week Tonight with John Oliver (HBO)*. [Online] Available at: https://www.youtube.com/watch?v=aRrDsbUdY_k&t=376s [Accessed 17 March 2019].

Ollivaud, P. & Turner, D., 2014. *The effect of the global financial crisis on OECD potential output*, s.l.: OECD Library.

Ølnes, S., Ubacht, J. & Janssen, M., 2017. Blockchain in government: Benefits and implications of distributed ledger. *Government Information Quarterly*, Volume 34, pp. 355-364.

O'Sullivan, K. P. V. & Kinsella, S., 2011. An institutional architecture for meta-risk regulation in Irish banking: Lessons from Anglo Irish Bank's Minsky moment. *Journal of Banking Regulation*, 12(4), pp. 342-355.

Panetta, K., 2018. *5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, 2018*. [Online] Available at: <https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/> [Accessed 23 February 2019].

Park, J. H. & Park, J. H., 2017. Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. *Symmetry*, 9(8), p. 13.

Perez, C., 2010. Technological revolutions and techno-economic paradigms. *Cambridge Journal of Economics*, 34(1), pp. 185-202.

Philippon, T. & Schnabl, P., 2013. Efficient recapitalization. *The Journal of Finance*, 68(1), pp. 1-42.

Pilkington, M., 2016. Blockchain technology: principles and applications. In: F. X. Olleros & M. Zhegu, eds. *Research Handbook on Digital Transformations*. Cheltenham: Edward Elgar, pp. 225-253.

Pitta, J., 1999. *Requiem for a Bright Idea*. [Online] Available at: <https://www.forbes.com/forbes/1999/1101/6411390a.html#167c3bf6715f> [Accessed 9 March 2019].

Prescott, E. S., 2004. Auditing and Bank Capital Regulation. *FRB Richmond Economic Quarterly*, 90(4), pp. 47-63.

Preston, H. H., 1933. The Banking Act of 1933. *The American Economic Review*, 23(4), pp. 585-607.

Ranganathan, S., George, A. D., Todd, R. W. & Chidester, M. C., 2001. Gossip-Style Failure Detection and Distributed Consensus for Scalable Heterogeneous Clusters. *Cluster Computing - The Journal of Networks, Software Tools and Applications*, 4(3), p. 197–209.

Rapoport, M. & McGinty, T., 2010. Still Broken: Banks Trim Debt, Obscuring Risks. *Wall Street Journal, Eastern edition*, 26 May, p. A.1.

Raskin, M., 2017. The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, pp. 305-341.

Rauchs, M. et al., 2018. *2nd Global Cryptoasset Benchmark Study*, Cambridge: University of Cambridge - Judge Business School - Centre for Alternative Finance.

Reidenberg, J. R., 1997. Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review*, 76(3), pp. 553-593.

Riccaboni, A., Giovannoni, E., Giorgi, A. & Moscadelli, S., 2006. Accounting and power: evidence from the fourteenth century. *Accounting History*, 11(1), pp. 41-62.

Romine, C., 2013. *Digital Signature Standard (DSS)*, Gaithersburg: National Institute of Standards and Technology.

Saad, M., Njilla, L., Kamhoua, C. & Mohaisen, A., 2019. *Countering Selfish Mining in Blockchains*. s.l., IEEE - International Conference on Computing, Networking and Communications (ICNC).

Saks, M. J., 1992. Do we really know anything about the behavior of the tort litigation system. And why not?. *University of Pennsylvania Law Review*, 140(4), pp. 1147-1292.

Sangster, A., 2016. The Genesis of Double Entry Bookkeeping. *The Accounting Review*, 91(1), pp. 299-315.

Schönhals, A., Hepp, T. & Gipp, B., 2018. Design Thinking using the Blockchain: Enable Traceability of Intellectual Property in Problem-Solving Processes for Open Innovation. In: *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*. Munich: ACM, pp. 105-110.

Schulze, H., 2018. *Insider Threat - 2018 Report*, s.l.: CA Technologies.

Schwartz, B. et al., 2008. *High Performance MySQL*. 2nd ed. Sebastopol: O'Reilly Media.

Securities and Exchange Commission, 2019. *Self-Regulatory Organizations; Cboe BZX Exchange, Inc.; Notice of Filing of Proposed Rule Change To List and Trade Shares of SolidX Bitcoin Shares Issued by the VanEck SolidX Bitcoin Trust, Under BZX Rule 14.11(e)(4), Commodity-Based Trust Shares*. [Online]

Available at: <https://www.federalregister.gov/documents/2019/02/20/2019-02732/self-regulatory-organizations-cboe-bzx-exchange-inc-notice-of-filing-of-proposed-rule-change-to-list>

[Accessed 18 March 2019].

Seibold, S. & Samman, G., 2016. *Blockchain Consensus: Immutable agreement for the Internet of value*, Hong Kong: KPMG.

Sharples, M. & Domingue, J., 2016. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. In: K. Verbert, M. Sharples & T. Klobučar, eds. *Adaptive and Adaptable Learning*. Lyon: Springer, pp. 490-496.

Shiller, R. J., 2008. *The Subprime Solution - How Today's Global Financial Crisis Happened, and What to Do about It*. 1st ed. Princeton: Princeton University Press.

Shughart, F. W., 1988. A Public Choice Perspective of the Banking Act of 1933. *Catp Kpirmaö*, 7(3), pp. 595-619.

Simser, J., 2015. Bitcoin and modern alchemy: in code we trust. *Journal of Financial Crime*, 22(2), pp. 156-169.

Sommers, K. & Conaughton, P., 2018. *Market Guide for Contract Life Cycle Management*. [Online]

Available at: <https://www.gartner.com/doc/reprints?id=1-5YJ91IV&ct=181218&st=sb>

[Accessed 31 March 2019].

Spengler, O., 1928. *The Decline of the West - Perspectives of World-History*. 1st ed. New York: Alfred A. Knopf.

Statista, 2019. *Ranking of the most popular database management systems worldwide, as of March 2019*. [Online]

Available at: <https://www.statista.com/statistics/809750/worldwide-popularity-ranking-database-management-systems/>

[Accessed 06 April 2019].

Swan, M., 2015. *Blockchain: Blueprint for a new economy*. 1st ed. s.l.:O'Reilly.

Swanson, T., 2015. *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems*, s.l.: R3 CEV.

Szabo, N., 1994. *Smart Contracts*. [Online]

Available at:

<https://web.archive.org/web/20160305205247/http://szabo.best.vwh.net/smart.contracts.html>

[Accessed 26 December 2018].

Szabo, N., 1997. Formalizing and securing relationships on public networks. *First Monday*, 2(9), p. 21.

Szabo, N., 1997. *The Idea of Smart Contracts*. [Online]

Available at:

<http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html>

[Accessed 28 December 2018].

The Editors of Encyclopaedia Britannica, 2018. *Bookkeeping (Encyclopaedia Britannica)*. [Online]

Available at: <https://www.britannica.com/topic/bookkeeping#ref286988>

[Accessed 29 December 2018].

The Institute of Chartered Accountants in England and Wales (ICAEW), 2010. *Audit of Banks: Lessons from the crisis*, London: ICAEW.

The World Bank, 2017a. *Population ages 65 and above (% of total)*. [Online]

Available at: <https://data.worldbank.org/indicator/SP.POP.65UP.TO.ZS?view=chart>

[Accessed 09th February 2019].

The World Bank, 2017b. *Population ages 15-64 (% of total)*. [Online]

Available at: <https://data.worldbank.org/indicator/SP.POP.1564.TO.ZS?view=chart>

[Accessed 09th February 2019].

The World Bank & International Monetary Fund, 2017. *Automated teller machines (ATMs) (per 100,000 adults)*. [Online]

Available at: <https://data.worldbank.org/indicator/fb.atm.totl.p5>

[Accessed 27th January 2019].

Treleaven, P., Gendal Brown, R. & Yang, D., 2017. Blockchain Technology in Finance. *Computer*, 50(9), pp. 14-17.

Trubek, D. M. et al., 1983. The Costs of Ordinary Litigation. *UCLA Law Review*, Volume 31, pp. 72-127.

Tschorsch, F. & Scheuermann, B., 2016. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, 18(3), pp. 2084-2123.

Tucker, A. W. & Straffin Jr., P. D., 1983. The mathematics of tucker: a sampler. *The Two-Year College Mathematics Journal*, 14(3), pp. 228-232.

Turing, A. M., 1937. On Computable Numbers, with an Application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, S2-42(1), pp. 230-265.

United Nations Population Division, 2017. *Population, total*. [Online]
Available at: <https://data.worldbank.org/indicator/SP.POP.TOTL?view=chart>
[Accessed 09th February 2019].

Valukas, A. R., 2010. *Lehman Brothers Holdings Inc. Chapter 11 Proceedings Examiner's Report*, New York: United States Bankruptcy Court - Southern District of New York.

Vanoli, A., 2005. *A History of National Accounting*. 1st ed. Amsterdam: IOS Press.

Vasek, M. & Moore, T., 2015. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. In: R. Böhm & T. Okamoto, eds. *Financial Cryptography and Data Security - 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers*. Berlin: Springer, pp. 44-61.

von Goethe, J. W., 1798. *Wilhelm Meister's Lehrjahre (Buch 1)*. [Online]
Available at: <https://www.gutenberg.org/cache/epub/2335/pg2335.html>
[Accessed 27 December 2018].

von Neumann, J., 1993. First draft of a report on the EDVAC. *IEEE Annals of the History of Computing*, 15(4), pp. 27-75.

Walport, S. M., 2016. *Distributed Ledger Technology: beyond block chain*, London: Government Office for Science.

Wang, B. et al., 2018. Large-scale Election Based On Blockchain. *Procedia Computer Science*, Volume 129, pp. 234-237.

Watanabe, H. et al., 2016. *Blockchain contract: Securing a Blockchain applied to smart contracts*. Las Vegas, IEEE.

Webel, B. & Labonte, M., 2018. *Costs of Government Interventions in Response to the Financial Crisis: A Retrospective*, Washington D.C.: Congressional Research Service.

Weber, M., 1981. *General Economic History*. New Brunswick: Transaction Publishers.

Wilson, T. & Wada, T., 2018. *Coincheck heist sheds light on Japan's rush to create cryptocurrency rules*. [Online]

Available at: <https://www.reuters.com/article/us-japan-cryptocurrency-regulation/coincheck-heist-sheds-light-on-japans-rush-to-create-cryptocurrency-rules-idUSKBN1FW04F>

[Accessed 11th November 2018].

Woodside, J. M., Augustine Jr., F. K. & Giberson, W., 2017. Blockchain Technology Adoption Status and Strategies. *Journal of International Technology and Information Management*, 26(2), pp. 65-93.

Wright, A. & De Filippi, P., 2015. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *SSRN Electronic Journal*, p. 58.

Xu, X. et al., 2017. *A taxonomy of Blockchain-Based Systems for Architecture Design*. Gothenburg, IEEE.

Yaga, D., Mell, P., Roby, N. & Scarfone, K., 2018. *Blockchain Technology Overview (NISTIR8202)*, Gaithersburg: National Institute of Standards and Technology.

Yamey, B. S., 1949. Scientific Bookkeeping and the Rise of Capitalism. *The Economic History Review*, 1(2/3), pp. 99-113.

Zheng, Z. et al., 2018. Blockchain Challenges and Opportunities: A Survey. *Int. J. Web and Grid Services*, 14(4), pp. 352-375.

Zheng, Z. et al., 2017. *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*. Honolulu, IEEE.

Zhou, J. & Gollmann, D., 1996. *A fair non-repudiation Protocol*. Oakland, IEEE.

Appendices

Appendix A

Year	FDIC insured institution	FDCI failed banks	Failure Rate
1990	15158	382	2.52%
1991	14482	271	1.87%
1992	13853	181	1.31%
1993	13221	50	0.38%
1994	12604	15	0.12%
1995	11971	8	0.07%
1996	11454	6	0.05%
1997	10923	1	0.01%
1998	10464	3	0.03%
1999	10222	8	0.08%
2000	9904	7	0.07%
2001	9614	4	0.04%
2002	9354	11	0.12%
2003	9181	3	0.03%
2004	8976	4	0.04%
2005	8833	0	0.00%
2006	8680	0	0.00%
2007	8534	3	0.04%
2008	8305	30	0.36%
2009	8012	148	1.85%
2010	7658	157	2.05%
2011	7357	92	1.25%
2012	7083	51	0.72%
2013	6812	24	0.35%
2014	6509	18	0.28%
2015	6182	8	0.13%
2016	5913	5	0.08%
2017	5670	8	0.14%

Table 3: U.S. Bank failure rate 1990 to 2017

Appendix B

Bank Name	Country	Closing date
<u>Parkhead Credit Union Limited</u>	United Kingdom	Apr-2019
<u>Greater Milton and Possilpark Credit Union Ltd</u>	United Kingdom	Mar-2019
<u>Independent Portfolio Managers Ltd</u>	United Kingdom	Dec-2018
<u>Qudos Insurance A/S</u>	United Kingdom	Dec-2018
<u>Horizon Insurance Company Ltd</u>	United Kingdom	Dec-2018
<u>K&C Credit Union Ltd</u>	United Kingdom	Oct-2018
<u>Dial-A-Cab Credit Union Ltd</u>	United Kingdom	Sep-2018
<u>Harp Credit Union Ltd</u>	United Kingdom	Sep-2018
<u>My Community Bank Wales</u>	United Kingdom	Aug-2018
<u>Alpha Insurance A/S</u>	United Kingdom	May-2018
<u>Beaufort Securities Ltd</u>	United Kingdom	Mar-2018
<u>Strand Capital Ltd</u>	United Kingdom	May-2017
<u>Gable Insurance AG</u>	United Kingdom	Nov-2016
<u>Enterprise Insurance Company Plc</u>	United Kingdom	Jul-2016
<u>UK Car Group Ltd</u>	United Kingdom	Dec-2015
<u>Balva AAS Insurance</u>	United Kingdom	Jul-2014
<u>European Risk Insurance Company hf.</u>	United Kingdom	Apr-2014
<u>Millburn Insurance Company Ltd</u>	United Kingdom	Dec-2013
<u>Hypo Alpe-Adria-Bank International</u>	Austria	Dec-2013
<u>SNS REAAL</u>	Netherlands	Feb-2013
<u>Sparekassen Lolland</u>	Denmark	Jan-2013
<u>Toender Bank</u>	Denmark	Nov-2012
<u>North Yorkshire Credit Union</u>	United Kingdom	Nov-2012
<u>Lemma Europe Insurance Company Limited</u>	United Kingdom	Oct-2012
<u>Tamworth Credit Union</u>	United Kingdom	Sep-2012
<u>TT Hellenic Postbank</u>	Greece	Aug-2012
<u>Waltonian Credit Union</u>	United Kingdom	Aug-2012
<u>Caixa Geral de Depósitos</u>	Portugal	Jun-2012
<u>Banco BPI</u>	Portugal	Jun-2012
<u>Millennium BCP</u>	Portugal	Jun-2012
<u>Norton Insurance Services Ltd</u>	United Kingdom	May-2012
<u>Alpha Bank</u>	Greece	May-2012
<u>T Bank</u>	Greece	May-2012
<u>Bankia</u>	Spain	May-2012
<u>Pallister Credit Union</u>	United Kingdom	May-2012
<u>Permanent TSB</u>	Ireland	Apr-2012
<u>Banca Network Investimenti</u>	Italy	Jan-2012

<u>Latvijas Krajbanka</u>	Latvia	Nov-2011
<u>Bankas Snoras AB</u>	Lithuania	Nov-2011
<u>Max Bank</u>	Denmark	Nov-2011
<u>Dexia</u>	Belgium	Oct-2011
<u>Fjordbank Mors</u>	Denmark	Aug-2011
<u>Crystal Clear Home Loans Ltd</u>	United Kingdom	Jul-2011
<u>Wilmslow Financial Services Plc</u>	United Kingdom	Jul-2011
<u>Irish Nationwide Building Society</u>	Ireland	Jul-2011
<u>Banca UBAE S.p.A.</u>	Italy	Jun-2011
<u>Welcome Financial Services Ltd</u>	United Kingdom	Mar-2011
<u>Amagerbanken</u>	Denmark	Feb-2011
<u>Havant Area Savers Credit Union</u>	United Kingdom	Jan-2011
<u>Keater Ltd</u>	United Kingdom	Dec-2010
<u>EBS Building Society</u>	Ireland	Dec-2010
<u>Bank of Ireland</u>	Ireland	Nov-2010
<u>The Exchange Insurance Company Ltd</u>	United Kingdom	Oct-2010
<u>Eik Bank</u>	Denmark	Sep-2010
<u>Allied Irish Bank</u>	Ireland	Aug-2010
<u>Caja Sur</u>	Spain	May-2010
<u>Bright Finance Ltd</u>	United Kingdom	Apr-2010
<u>Sofia Bank</u>	Finland	Mar-2010
<u>Capinordic A/S</u>	Denmark	Feb-2010
<u>Presbyterian Mutual Society</u>	United Kingdom	Jan-2010
<u>Chelsea Building Society</u>	United Kingdom	Dec-2009
<u>The Aldgate Insurance Company Ltd</u>	United Kingdom	Nov-2009
<u>Promise Finance Ltd</u>	United Kingdom	Oct-2009
<u>Picture Financial Services Plc</u>	United Kingdom	Jul-2009
<u>Eurolife Assurance (International)Ltd</u>	United Kingdom	Apr-2009
<u>Caja Castilla La Mancha</u>	Spain	Apr-2009
<u>Dunfermline Building Society</u>	United Kingdom	Mar-2009
<u>Banco Popolare</u>	Italy	Mar-2009
<u>Straumur Burdaras</u>	Iceland	Mar-2009
<u>Fionia Bank</u>	Denmark	Feb-2009
<u>Anglo Irish Bank</u>	Ireland	Jan-2009
<u>London Scottish Bank</u>	United Kingdom	Dec-2008
<u>Royal Bank of Scotland Group</u>	United Kingdom	Nov-2008
<u>EBH Bank</u>	Denmark	Nov-2008
<u>Parex Bank</u>	Latvia	Nov-2008
<u>Kommunalkredit/KA Finanzbank</u>	Austria	Nov-2008
<u>Barnsley Building Society</u>	United Kingdom	Oct-2008
<u>Landsbanki</u>	Iceland	Oct-2008

<u>Bradford & Bingley</u>	United Kingdom	Oct-2008
<u>Glitnir Bank</u>	Iceland	Sep-2008
<u>Fortis Netherlands & Belgium</u>	Netherlands & Belgium	Sep-2008
<u>Halifax Bank of Scotland</u>	United Kingdom	Sep-2008
<u>Hypo Real Estate Holding AG</u>	Germany	Sep-2008
<u>Kaupthing</u>	Iceland	Sep-2008
<u>Roskilde Bank</u>	Denmark	Aug-2008
<u>Northern Rock</u>	United Kingdom	Feb-2008
<u>Highlands Insurance Company (UK) Ltd</u>	United Kingdom	Nov-2007
<u>AA Mutual International Insurance Services Ltd</u>	United Kingdom	May-2007

Appendix C

CobbleStone Software	CobbleStone Contract Insight Enterprise Edition
Exari	Exari Contracts
SAP Ariba	SAP Ariba Contracts
Symfact	Symfact Contract and Compliance Software Portal
Thomson Reuters	Thomson Reuters Contract Express

[Based on Sommers & Conaughton (2018)]