

PERMISSIONED BLOCKCHAINS AS  
OWNERSHIP-REGISTRATION SYSTEMS

**MASTER'S THESIS**

**ROBERT DIEBELS**

JUNE, 2017

AS PART OF A MASTER'S GRADUATE PROJECT AT THE UNIVERSITEIT VAN  
AMSTERDAM

**Supervisor:** M. X. Makkes, Postdoctoral researcher, Vrije Universiteit

## Abstract

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
1.1	Bitcoin . . . . .	2
1.2	Blockchains . . . . .	2
1.3	Thesis . . . . .	3
1.4	Contributions . . . . .	3
<b>2</b>	<b>Literature Survey</b>	<b>4</b>
2.1	Methodology . . . . .	4
2.2	Scope . . . . .	4
2.3	Results . . . . .	5
2.4	Conclusion . . . . .	5
<b>3</b>	<b>Research methodology</b>	<b>7</b>
3.1	Primary research questions . . . . .	7
<b>4</b>	<b>Implementation</b>	<b>8</b>
<b>5</b>	<b>Evaluation</b>	<b>9</b>
<b>6</b>	<b>Conclusion</b>	<b>10</b>

# Chapter 1

## Introduction

\*Write a lead\*

### 1.1 Bitcoin

In 2008 a scientist or group of scientists under the pseudonym Satoshi Nakamoto published a paper[4] describing a combination of technologies enabling transfer of currency without an intermediate third party known as Bitcoin. In this system each party wishing to exchange currency is required to become a node in a peer-to-peer network and keep a record of all transactions executed to-date. In accounting this type of record-keeping used to be done in books known as ledgers. A system which distributes records to a set of nodes on a network is commonly known as a distributed ledger. The key novelty in Bitcoin as opposed to earlier implementations of distributed ledgers lies in how it solved the double-spending problem.

The problem concerns a currency transfer with a minimum of 2 parties, a sender and a recipient. For a sender to send a certain amount of cash to a recipient she must have enough currency to do so. In a digital environment where currencies are non-physical, this is ensured by keeping track of the balance of a senders' currency. Should a sender have malicious intent and try to "double-spend" a certain amount the third party blocks the attempt enabling trust between all parties exchanging via the third party.

Bitcoin resolves the double-spending problem with two parallel processes operating on a distributed ledger. A process which ensures transactions are valid and a process called mining where nodes in the network gather sets of validated transactions into blocks. Each block contains a references to the previously mined block forming a chain of blocks. As an incentive to mine blocks a node receives a reward after successfully mining a block. The node is rewarded in the form of a Bitcoin, the currency which is transferred between participating parties in the Bitcoin peer-to-peer network.

### 1.2 Blockchains

Named after the chain of blocks used by Bitcoin, the combination of technologies that underlie Bitcoin have become known as blockchain-technology or sim-

ply blockchain. The solutions blockchains can offer are applicable to a wider spectrum than currency transactions alone. The technology can be a replacement to many systems where an intermediate party is responsible for transfer of digital assets between two other parties. For instance, contrary to unpermissioned blockchains like Bitcoin, where anyone can participate, there are situations where blockchains are applicable where participants need to meet certain requirements before they can access or submit transactions. Blockchains which have enabled such access control are referred to as permissioned blockchains.

Permissioned blockchains offer advantages over unpermissioned blockchains. In an environment where access control is in place the governing agent might require identification of participants in the "real-world". Lowering the chance that there will be malicious nodes in the blockchain network requiring less validation of transactions, since tampering with records will be less appealing. As a consequence the leniency in checking transactions and blocks improves the throughput of the blockchain.

### 1.3 Thesis

Blockchains have a high problem-solving potential [3] even-though the technology is still lacking in certain areas [6] [7]. Permissioned blockchains in particular have not received much attention concerning comparison with the current market systems they can replace [2].

In this thesis a use-case set in the music-industry is explored through implementation of a rights-holder registration system in currently existing permissioned blockchains. These implementations are then compared to one another and the in-use systems. The comparative experiment that was performed as part of the Thesis focused on throughput as it's primary measure.

### 1.4 Contributions

The primary contributions of this Thesis are:

- A mapping study on the current state of research on permissioned blockchains.
- Implementation of a music-industry use-case in several permissioned blockchains.
- Permissioned blockchain performance evaluation through a controlled experiment.

## Chapter 2

# Literature Survey

Examining the current body of knowledge on permissioned blockchains was done by conducting a mapping study [2] based on [6] and [5]. This chapter serves as a summary outlining the study's methodology, scope and findings. The full study is available on GitHub<sup>1</sup>.

### 2.1 Methodology

A mapping study for software engineering as designed by [5] consists of; (1) a scope definition by a set of research questions, (2) conduction of a search based on defined search terms, (3) a search result screening by applying exclusion and inclusion criteria, (4) classification of results through abstract key-wording, (5) data extraction based on a set of data extraction items. Here the term "results" was broadened to include scientific studies and implementations of permissioned blockchains accommodating the study's research questions.

### 2.2 Scope

The scope of the study was limited by the definition of a set or research questions. Serving the purpose of examining the current state of permissioned blockchain literature, identifying existing permissioned blockchain implementations, assessing empirical evidence gathering in literature and practice and lastly serving to identify research of permissioned blockchains in the context of the music-industry. The following research questions detail the question and why it was of importance to answer for the purpose of this Thesis.

**Which topics are addressed in current research on permissioned blockchains?** Answering this question is important to assess which topics are being researched. This will help judge to what degree the graduate project can contribute to the field.

---

<sup>1</sup><https://github.com/RobertDiebels/graduate-project/blob/master/dist/experiment.pdf>

**What implementations of permissioned blockchains exist?** Evaluating which permissioned blockchains exist and what flaws they have will help assessing the state of current permissioned blockchain technology. In turn this can create a framework for which measurements should be performed when assessing a permissioned blockchain.

**What experiments are being performed on permissioned blockchains?** Assessing which experiments are performed on permissioned blockchains allows determining what the state of empirical evidence gathering in the field is. This will advance future experiments by providing an overview of which measurements are deemed valuable.

**Is there any research on blockchains related to the music-industry?** This question is relevant for the graduate projects' topic, relevancy and potential contributions to the field.

## 2.3 Results

The results of the survey showed that there is a focus on reporting on permissioned blockchains and improving the technology. With respectively 28% reporting and 48% suggesting improvements. Surprisingly only 43.8% of the research which suggested solutions or improvements did any experimentation and it was solely aimed at validating a suggested application or improvement. Search results for permissioned blockchain implementations revealed 7 blockchain implementations and 2 implementations with blockchain-like properties. A total of 8 implementations allowed for permissioning access.

## 2.4 Conclusion

Based on the survey's results we reach the following primary findings [2, p.16].

**Blockchain research lacks comparative research** Current literature is focused on improving several flaws in blockchain-technology. Such as privacy-preservation, consensus protocols, access control and more. The improvements suggested in these studies are then evaluated with the use of experimentation. This survey found no comparative research on improvements addressing the same flaw.

**Blockchain research lacks research aimed at reproduction of results** The results of this survey indicate that there is a lack of reproducing results of previous studies. In fact there was not one study aimed at reproducing results of other studies. The field could benefit from validating earlier research addressing and identifying flaws in experimental design.

**Blockchain research lacks use-case specific research** To validate the usefulness of blockchain technology it needs to be implemented and used. The survey identified several articles which suggest potential use-cases yet provide no implementation [1] [8].

**Blockchain research lacks evaluation of current implementations** The literature survey results indicate that implementations of blockchains have

not been objectively evaluated. Comparison of implementations could provide insights into general blockchain flaws and the suggestion of new improvements.

These findings indicate that the Thesis's aim is of value to the field and that several contributions can be made by performing a comparative experiment between current permissioned blockchains.



## Chapter 3

# Research methodology

\*lead\* \*hypothesis\*

### 3.1 Primary research questions

## Chapter 4

# Implementation

1. Corda
2. Hyperledger Fabric
3. Monax Tendermint

## Chapter 5

# Evaluation

## Chapter 6

## Conclusion

# Bibliography

- [1] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. Medrec: Using blockchain for medical data access and permission management. In *Open and Big Data (OBD), International Conference on*, pages 25–30. IEEE, 2016.
- [2] Robert Diebels. Literature survey - ownership using permissioned blockchains, 2017. Available at <https://github.com/RobertDiebels/graduate-project/blob/master/dist/survey.pdf>.
- [3] Juri Mattila et al. The blockchain phenomenon—the disruptive potential of distributed consensus architectures. Technical report, The Research Institute of the Finnish Economy, 2016.
- [4] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
- [5] Kai Petersen, Robert Feldt, Shahid Mujtaba, and Michael Mattsson. Systematic mapping studies in software engineering. In *EASE*, volume 8, pages 68–77, 2008.
- [6] Jesse Yli-Huumo, Deokyeon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. Where is current research on blockchain technology?—a systematic review. *PloS one*, 11(10):e0163477, 2016.
- [7] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, and Huaimin Wang. Blockchain challenges and opportunities: A survey. 2016.
- [8] Guy Zyskind, Oz Nathan, and Alex Pentland. Enigma: Decentralized computation platform with guaranteed privacy. *arXiv preprint arXiv:1506.03471*, 2015.