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

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[5] 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 simply 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 [4] even-though the technology is still lacking in certain areas [8] [9]. Permissioned blockchains in particular have not received much attention concerning comparison with the current market systems they can replace [3].

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 [3] based on [8] and [7]. This chapter serves as a summary outlining the study's methodology, scope and findings. The full study is available on GitHub[1].

2.1 Methodology

A mapping study for software engineering as designed by [7] 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.

[1] `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 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 [3, 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] [10].

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

This chapter defines the research methodology used in this Thesis. The sections in this chapter outline the graduate projects' hypothesis, research questions for evaluation of the hypothesis, an experimental design to answer said questions and how data gathered from the experiment is to be analysed.

3.1 Hypothesis

"Permissioned blockchains outperform current ownership-validation systems in terms of throughput and verification-speed."

3.2 Primary research questions

How well do blockchains perform in permissioned environments compared to current systems? This question is answered via a comparative experiment detailed in the next section. The comparative experiment is used to gauge permissioned blockchain performance compared to current systems and each other.

What measurements should be taken to compare permissioned blockchains? Comparing several permissioned blockchain implementations can only be done by comparing them based on a unit of measurement. Which units should be measured and why?

3.3 Experimental design

The experimental design described in this section is largely based on the design by [2, p.64]. The version of the design defined in this Thesis examines a Performing Rights Organizations (PROs) use-case implemented in several permissioned blockchains. It is useful to read the

3.4 Result analysis

Chapter 4

Implementation

1. Corda
2. Hyperledger Fabric
3. Monax Tendermint

Chapter 5

Use-case

This chapter describes the use-case under examination in this Thesis. To gain an understanding of the PROs use-case several representatives of Dutch PROs were interviewed about current business processes and data-flow. Using their answers this chapter sets out to, clarify their use-case, identify entities operating with their business in section 5.2, model current PROs processes using Business Process Modelling (BPM) in section 5.3 and show how blockchains may benefit PROs in section 5.4.

5.1 Introduction

Under most legal systems in the world the creation of a work of art endows its creator with rights of ownership. Depending on the legal system this includes licensing other parties to use the work under a set of usage terms, often entailing monetary payments. In most cases a works' rights-holder wants assurance of payment by licensees. In the context of the music-industry ensuring payment is received is done by Performing Rights Organizations (PROs).

In the Netherlands PROs are by default non-profit foundations, the members of which are creators of musical works. Acting as a representative of a creator the foundation administrates and processes usage of works. Usage data is processed and rights-holders of a work receive payment.

5.2 Entities

This section specifies the entities which drive the PROs use-case. The entities consist of (1) rights-holders such as artists, composers and producers, (2) licensees such as the radio and television industry, the hospitality industry and Digital Service Providers (DSPs), (3) Performing Rights Organizations (PROs) who act as intermediaries between rights-holders and licensees.

5.3 Business Process Model

This section defines a BPM diagram of the PROs use-case. The diagram as shown in Figure 5.1 shows an abstraction of the processes within Bureau voor

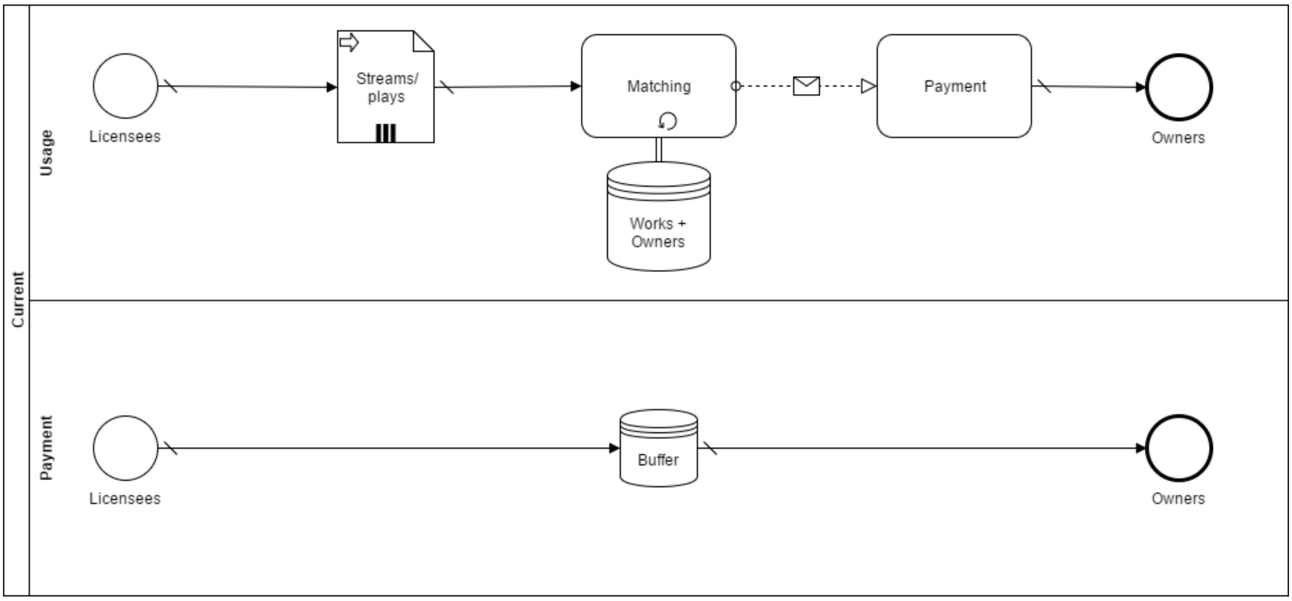

Figure 5.1: BPM of current PROs business processes.

Muziek-Auteursrechten (Buma) Stichting tot Exploitatie van Mechanische Reproduktierechten voor Auteurs (Stemra) (Buma/Stemra) and Stichting ter Exploitatie van Naburige rechten (SENA).

The first lane in the diagram shows a process model in which (1) data is provided to PROs by licensees describing which works were played or streamed, (2) the works found in the data are identified through a matching process, (3) and a payment process for rights-holders. The second lane shows a parallel process were licensees transfer payment to a PRO. Payment is buffered and once the processes in the first lane are complete payments are made.

5.4 Blockchain

According to [6, p.8] blockchains can provide the record-industry with (1) A networked database for music copyright information (2) Fast, friction-less royalty payments (3) Transparency through the value chain (4) and access to alternative sources of capital. The interviewed PROs agree with this observation. Stating that their primary motivations for using blockchains are improving operational transparency towards their members and the possibility of friction-less royalty payments.

Adjusting the model defined in Figure 5.1 for usage with a blockchain yields the model depicted in Figure 5.2. The model shows that the usage process is simplified by (1) allowing licensees to transfer usage data directly to the blockchain, (2) avoiding the matching process between PRO data and usage data (3) and subsequently, faster payment through a process tied into the blockchain. The payment process would be sped up significantly by avoiding the matching process though its structure would remain similar to the original. As instant payments would require owners and licensees to predetermine prices for usage.

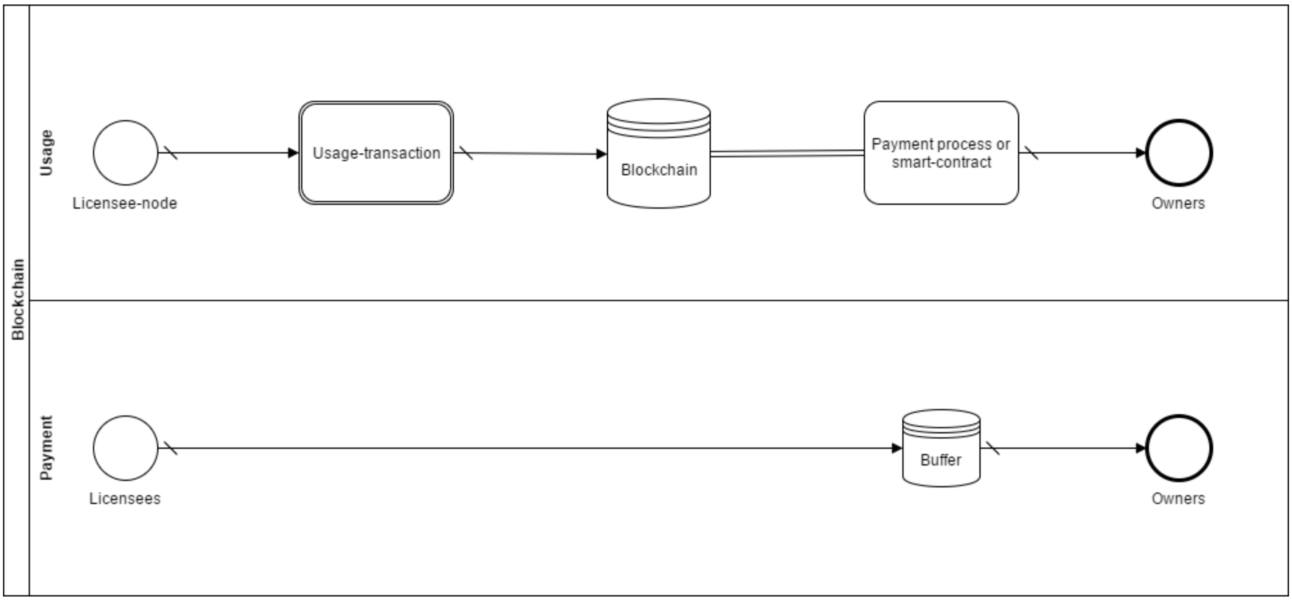

Figure 5.2: BPM of current PROs business processes.

Considering current market conditions interviewed PROs found it unlikely that licensees would be willing to put a price on the usage of a single work. Their reasoning was that larger DSPs would have to charge their users for usage of individual works. Their current business model involves a fixed monthly fee for all users, introducing pricing of individual works would complicate their model significantly.

5.5 Conclusion

The definition of the Performing Rights Organizations (PROs) use-case provided in this chapter shows that current PRO processes can be optimized by forgoing the need to match input data to stored data within the system. Blockchains can provide significant improvements to current processes. Most notable are the simplification, removal of obsolete processes and inherent properties of blockchains such as transparency of PRO operation.

Chapter 6

Evaluation

Chapter 7

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] Ethan Buchman. *Tendermint: Byzantine Fault Tolerance in the Age of Blockchains*. PhD thesis, 2016.

[3] Robert Diebels. Literature survey - ownership using persmissioned blockchains, 2017. Available at `https://github.com/RobertDiebels/graduate-project/blob/master/dist/survey.pdf`.

[4] Juri Mattila et al. The blockchain phenomenon–the disruptive potential of distributed consensus architectures. Technical report, The Research Institute of the Finnish Economy, 2016.

[5] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[6] Marcus O'Dair, Zuleika Beaven, David Neilson, Richard Osborne, and Paul Pacifico. Music on the blockchain. 2016.

[7] Kai Petersen, Robert Feldt, Shahid Mujtaba, and Michael Mattsson. Systematic mapping studies in software engineering. In *EASE*, volume 8, pages 68–77, 2008.

[8] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. Where is current research on blockchain technology?—a systematic review. *PloS one*, 11(10):e0163477, 2016.

[9] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, and Huaimin Wang. Blockchain challenges and opportunities: A survey. 2016.

[10] Guy Zyskind, Oz Nathan, and Alex Pentland. Enigma: Decentralized computation platform with guaranteed privacy. *arXiv preprint arXiv:1506.03471*, 2015.