WORKING TITLE: Ownership in permissioned blockchains
- A rights distribution use-case -

Robert Diebels

As part of the Master Software Engineering
at the University of Amsterdam

May, 2017

1 Contact information

This section contains contact information about student, host company and supervisors.

Name	Robert Diebels
Primary email-address	robertdiebels@gmail.com
Secondary email-address	...
Phone	Request by email
Address	Binnenhof 205, 1412 LA, Naarden
Website	`http://www.robertdiebels.com`

Table 1: Student

This graduate project has no host-company.

Table 2: Host company

Name	Marc Makkes
Primary email-address	m.x.makkes@vu.nl
Secondary email-address	...
Function	Postdoctoral Researcher
Phone	Request by email
Address	Boelelaan 1081, 108 HV, Amsterdam
Website	...

Table 3: Supervisor

2 Introduction

The graduate project proposed in this article is part of a larger research project on protocols for permission blockchains at the Vrije Universiteit (VU). Several parties from the music-industry are interested in permissioned blockchains as the technology has the potential to increase the efficiency of their businesses.

The music-industry's business model is based on payment for usage of musical works to rights-holders. Enforcing the business model involves verifying and validating: (1) users of a musical work transfer payment, (2) correct amounts are being transferred, (3) the correct rights-holders receive payment and (4) that assumed rights-holders are in fact hold rights to a musical work. This validation and verification is performed by Performing Rights Organizations (PROs) who act on behalf of rights-holders.

Solutions enabling this business model often use centralized systems to validate ownership and distribute payment. These systems grow in size and complexity as time passes. Even requiring humans to manually validate ownership before records of ownership are entered into the system. The records in these centralized systems are often duplicated by other PROs as they are unaware of what records their counterparts have.

In theory permissioned blockchains are perfectly suited to solve these issues. As their clients/protocols have access control mechanisms which ensure specified conditions are met before a client can access records in the system. The graduate project aims to implement the music industry's requirements in several existing permissioned blockchains. Then use these implementations in a comparative experiment for evaluation of permissioned blockchains capabilities compared to current systems.

Parties directly involved in the over-arching research project include: Stichting ter Exploitatie van Naburige rechten (SENA), Bureau voor Muziek-Auteursrechten (Buma) Stichting tot Exploitatie van Mechanische Reproduktierechten voor Auteurs (Stemra) (Buma/Stemra) and the VU. SENA and Buma/Stemra are PROs which help artists collect payment for their works and performances. The scope of interested parties isn't limited to those mentioned as there are many use-cases where an authority needs to impose rules on a group of identified clients.

The article contains the following sections. In section 3 the graduate-projects' composition is explained, a problem analysis is described concerning the PROs use-case, a solution using permissioned blockchains is suggested, a hypothesis is formed and the means to evaluate it are detailed. Ensuring the graduate-project contributes to the field was done by performing a literature survey. Its findings are reported in section 4. Finally, section 5 concludes which the contributions the proposed graduate-project would make to the field.

3 Graduate-project composition

This section explores the graduate projects' composition. What is the exact problem being addressed and how can permissioned blockchains solve this problem?

3.1 Problem analysis

In the music-industry there are organizations known as Performing Rights Organizations (PROs). These organizations ensure that artists, performers and writers receive payment when musical works they have created are used. Their tasks can be summarized as ensuring that: (1) users of a musical work transfer payment, (2) correct amounts are being transferred, (3) the correct rights-holders receive payment and (4) that assumed rights-holders are in fact hold rights to a musical work. Currently these tasks are time-consuming sometimes resulting in payments being delayed for over a year, as collected payments are distributed 1 to 4 times a year. It would be preferable to distribute payments instantly upon usage or at the very least more frequently.

A solution to these efficiency problems can be offered by blockchains. Blockchain-technology was first introduced in [3] by an author or authors under the pseudonym "Satoshi Nakamoto". Properties of blockchains such as automatic verification of transactions and code which autonomously operates on the blockchain could alleviate the performance and efficiency issues the music-industry has with current systems. Concerning the PROs use-case blockchains which regulate who can perform transactions on a blockchain are of interest. As verification needs to take place to assure rights-holders have been identified prior to being admitted to the blockchain and eligible to receive payments.

The aim of the proposed graduate project is the evaluation of the current state of permissioned blockchain implementations. This is achieved by designing an experiment evaluating performance and comparing it to each blockchain and current systems used by PROs. As such the problem being addressed by the proposed graduate project is one of permissioned blockchain performance and efficiency.

3.2 Hypothesis

A permissioned blockchain enforces access control ensuring that the nodes in the network adhere to certain rules. In the case of rights distribution and ownership-validation this means that the certain nodes must be known and have a verified identity. Blockchains have certain properties which help solve this issue.

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

3.3 Research method

Evaluation of the proposed graduate-projects' hypothesis is achieved by employing a comparative methodology. The PRO use-case will be implemented in currently available permissioned blockchains. Implementations of the use-case will be used in a comparative experiment. Data gathered from the experiment

is then used for a comparison of current systems and different types of permissioned blockchain implementations.

3.4 Research questions

3.4.1 Primary

How well do blockchains perform in permissioned environments compared to current systems? The aim of the proposed graduation project is to design and perform an experiment on several permissioned blockchains. 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?

3.4.2 Secondary

How would a permissioned blockchain implement ownership-validation? Transactions are addressed to a public key. Owners who can provide a digital signature signed with their private key show that they are the entity to which a transaction is addressed. This is can serve as a proof-of-ownership.

This type of ownership-validation becomes rather interesting with regard to local copies of a blockchain. If a property is stored on the chain it becomes possible to validate usage instantly. As a result each local copy would become extraordinarily large. How would a blockchain implement ownership-validation without inflating the chain?

How does a permissioned blockchain verify the legitimacy of ownership? A permissioned blockchain would have a mechanism in place to limit entry to the network. When a new client (artist) creates a legitimate new work can they join the network without a need for verification? How limiting should a permissioned blockchain be?

How would the blockchain handle multiple owners of a property? If there are works which have collaborators they are entitled to their share of ownership. Simply registering multiple public keys as owners would not suffice as some entities may have had a bigger share in the creation of the work.

How would ownership-transfer be performed in a permissioned blockchain? Are blockchains capable of handling cases in which ownership-transfer need to take place? If so, what would examples of mechanisms to do this?

How would the blockchain handle contesting of ownership? If an artist does not reside on the chain, how can it be avoided works they created end up on the chain? As they would contest ownership the moment they do enter the chain. This would also apply to works they collaborated on which are on the chain.

3.5 Expected results

The following list shows the projects' expected results.

- Main: Evaluation of permissioned blockchain capabilities and restrictions.
- Implemented use-case in one or more permissioned blockchains.
- Implementations are use-able for experimentation.
- Implementations are used in comparative experiment.
- Experiment results are used to evaluate hypothesis.

3.6 Experiment

Evaluating the hypothesis is achieved by defining an experiment which fits it. The experiment proposed to accomplish this is based on [1]. It defines several experiments run on the Tendermint consensus protocol and measurements of transactions per second (Tx/s) and block formation per second (Bf/s).

The experiment proposed for the graduate project is described in full in a separate document available on GitHub.

3.7 Required expertise

Completion of the Master project and the accompanying research require the acquisition of the following expertise.

Blockchain knowledge Expertise on blockchain technology, its faults and its benefits needs to be acquired.

Ownership The concept of ownership and how to implement it in a blockchain.

Requirements gathering Requirements gathering needs to be performed to elicit the wishes of SENA and Buma/Stemra.

Java Programming Depending on the outcomes of several research questions a permissioned blockchain is chosen and adjusted to fit the needs of the use-case. Preferably this is built using Java.

Blockchains Knowledge on the types of blockchains that are available needs to be gained. Their flaws and strengths should also be known.

3.8 Risks

Possible risks to the master project are listed and explained below.

Relatively new research subject This may negatively influence the proposed graduate-project. As the total body of knowledge is relatively small.

Possible lack of comparison data This depends on the state of in-use systems of SENA and Buma/Stemra. If there is a relatively small amount of data available on performance of current processes and systems gathering them may have occur. If there is none, the Proof of Concept (PoC) should have different variations.

Personal mathematical expertise The author's mathematical skill-set is sufficient for most problems. However, most encryption algorithms or concepts rely on difficult to solve mathematical problems. The author recognizes that his skill-set in mathematics may be a roadblock to understanding these fundamentals. The question is whether or not the graduate-project will touch upon those subjects.

3.9 Timeline

- Feb. 28, 2017 - Meeting with SENA, present preliminary project proposal.
- Apr. 1-31, 2017 - Finish survey.
- May. 1-31, 2017 - Complete experimental design.
- May. 20-22, 2017 - Select permissioned blockchain implementations for experimentation.
- May. 20-31, 2017 - Complete data and requirements gathering from SENA and Buma/Stemra.
- May. 22-31, 2017 - Research development details of selected implementations.
- Jun. 1-30, 2017 - Write implementations of selected permissioned blockchain and run experiment.
- Jul. 1-31, 2017 - Analyse experiment results, write and submit Thesis.

4 Literature survey

Ensuring the proposals' validity was done by performing a survey of current literature on permissioned blockchains. This section summarizes the findings of that survey and uses those findings to ensure the proposal explores a legitimate need for blockchain research. The full survey can be found on GitHub.

4.1 Findings

The results of the survey indicate that a majority of the research done on permissioned blockchains concerns mapping its current state or providing solutions to current flaws.

"With respectively 28% reporting and 48% suggesting improvements. Surprisingly only 43.8%of the research which suggested solutions or improvements did any exper-imentation and it was solely aimed at validating a suggested application or improvement."[2, p.1]

4.2 Proposal validity

The survey sought to answer 4 research questions which can be found in [2]. Out of the 4 research questions asked and answered in [2] 2 in particular are worth addressing mentioning as their conclusions lead to support for the graduate projects' main goal.

RQ3 - What experiments are being performed on permissioned blockchains? The mapping study included 25 articles for analysis. Out of those 25 only 7 contained a form of controlled experiment. None of which analysed current implementations or replicated earlier experiments.

RQ4 - Is there any research on blockchains related to the music-industry? The survey found only 1 article aimed at summarizing and explaining why blockchains are potentially useful for usage by PROs. In [4] the potential benefits of blockchains are summarized as: (1) a networked database for music copyright information, (2) fast, frictionless royalty payments, (3) transparency through the value chain, (4) access to alternative sources of capital. Which is backed by SENAs and Buma/Stemra which have reported similar interests and benefits.

The article does not evaluate any empirical findings related to implementation of music-industry use-cases and blockchains.

The findings concerning both these research questions indicate that performing a thorough comparative experiment using the PROs use-case can contribute to the field.

5 Conclusion

This proposal aimed at providing insight into a Software Engineering Master graduate-project. The proposed graduate-project would provide insights into the state of current permissioned blockchain implementations by designing an experiment for a use-case provided by several Performing Rights Organizations (PROs).

Current literature was assessed for possible contributions with a survey [2] in the form of a systematic mapping study. The possible contributions the graduate-project could make were derived from that survey and are listed below.

Empirical research on current current permissioned blockchain implementations is needed The mapping study revealed a lack of controlled experimentation and no comparative research. A comparative experiment as suggested in this proposal would be a significant contribution to the field.

Use-case studies for permissioned blockchains can contribute to the field The implementation of a use-case like that of the PROs in permissioned blockchains can provide concrete insight into the capabilities of permissioned blockchains.

An evaluation of permissioned blockchains capabilities for the music-industry contributes to both area's of research As mentioned in [4] blockchains can potentially provide benefits to the music-industry. The implementation of the PROs use-case in several permissioned blockchains contributes to both fields by evaluating performance compared to current systems.
The author believes that these contributions support the pursuance of a Thesis exploring problem described in this proposal.

References

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

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

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

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

Acronyms

Buma Bureau voor Muziek-Auteursrechten. 2

Buma/Stemra Buma Stemra. 2, 5–7

PoC Proof of Concept. 2, 3, 5, 6

PRO Performing Rights Organization. 2, 3, 7

SENA Stichting ter Exploitatie van Naburige rechten. 2, 5–7

Stemra Stichting tot Exploitatie van Mechanische Reproduktierechten voor Auteurs. 2

VU Vrije Universiteit. 2