Permissioned Blockchain Partitioning: Is It Useful?

Proposal

Robert Diebels
October, 2018

As part of a Master's Degree graduate project at the University of Amsterdam

Supervisor: M. X. Makkes, PhD., Vrije Universiteit.

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

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.

However, the throughput of permissioned blockchains can be further improved upon. As even permissioned blockchains do not always perform as well as current centralized solutions. Considering this throughput problem this document describes a proposal for an experiment comparing two variants of a permissioned blockchain. The first variant is a single permissioned blockchain, the second an in-tree rooted-tree variant in which several smaller blockchains are connected and transactions are propagated from these networks to a root-network. This partitioned rooted-tree variant should significantly improve performance. As transactions can now be performed in parallel by sending them to one of the smaller leaf-networks based on a predefined limitation, whereas a single network process all transactions.

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.

This proposal 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 Performing Rights Organizations (PROs) ensure that artists, performers and writers receive payment when musical works they have created are used. The tasks of PROs 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, (4) that assumed rights-holders are in fact hold rights to a musical work and (5) keeping track of which tracks have been played and by whom. 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] 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. For the PROs use-case blockchains which limit who can perform transactions on a blockchain are of interest.

This area of interest is covered by permissioned blockchains such as Hyperledger Fabric. Unfortunately, even permissioned blockchains suffer from performance issues. Hyperledger Fabric for instance is incapable of reaching a throughput higher than 140 Transactions per second (Tx/s) [5, p. 5]. A solution to these performance issues would be to execute the transactions in parallel by creating several smaller permissioned blockchains in a rooted-tree configuration. Another name for this process is partitioning. In this proposal we would be partitioning a blockchain into several smaller blockchains. Where each blockchain would then be limited for use to a unique set of users.

This set of users could for instance, be limited based on geo-spatial location. Take a country such as the Netherlands which consists of 12 provinces. A rooted-tree configuration of the Netherlands would then consist of 13 blockchains. Each province represented by one blockchain and the whole country would also be represented by one.

The aim of the proposed graduate project is the evaluation of the performance of a single permissioned blockchain versus an in-tree rooted-tree variant of that blockchain. This is achieved by designing an experiment evaluating performance of both variants and comparing them to one-another. As such the problem being addressed by the proposed graduate project is one concerning permissioned blockchain performance and efficiency.

3.2 Hypothesis

Single permissioned blockchains handle transactions in a serial manner. This limits their capability to handle large amounts of transactions at a time. A

rooted-tree variant does not share these limitations because it consists of multiple blockchains operating in parallel. Due to this parallelization my Hypothesis is as follows:

Hypothesis In-tree rooted-tree permissioned blockchain networks outperform single permissioned blockchains.

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 by generating transactions for the amount of times a track has been played. Single and rooted-tree variants of the use-case developed in a permissioned blockchain will be used in a comparative experiment. The data gathered from the experiment will then be used for a comparison of a single permissioned blockchain and a rooted-tree variant.

3.4 Research questions

3.4.1 Primary

RQ1: How well does a single permissioned blockchain perform compared to a rooted-tree variant of that blockchain? The aim of the proposed graduation project is to design and perform an experiment on two variants of a permissioned blockchain single and rooted-tree. The comparative experiment is used to gauge a single permissioned blockchain performance with a rooted-tree variant of that blockchain.

3.4.2 Secondary

SRQ1: Which permissioned blockchain should be examined? Determining which permissioned blockchain is examined is pivotal for the relevance of the project. Examining frequently used permissioned blockchains are preferable over less used ones since their performance or lack thereof would impact more end-users.

SRQ2: What are the dependent variables for a comparison of performance between blockchain variants? For a comparison between variants of a blockchain to have any relevance a common denominator must be established. Which measurements can be taken and why are they suitable.

SRQ3: What are the independent variables that should be manipulated to assess performance of a permissioned blockchain? Depending on the change of input values a single permissioned blockchain may outperform a rooted-tree variant or vice-versa. Knowing which variables, if any, to manipulate impacts the relevance of the research.

SRQ4: How do we create a reproducible experiment for blockchain networks? For a comparative experiment to have value we need to be able to reproduce it.

SRQ5: How well does a single permissioned blockchain perform? Determining the performance of a single permissioned blockchain based on the determined measurements and input variables, is required in establishing a comparison between a single permissioned blockchain and a rooted-tree variant.

SRQ6: How well does a rooted-tree permissioned blockchain variant perform? Determining the performance of a rooted-tree permissioned blockchain variant based on the determined measurements and input variables, is required in establishing a comparison between a single permissioned blockchain and a rooted-tree variant.

3.5 Expected results

The following list shows the projects' expected results.

- Main: Evaluation of permissioned blockchain performance vs. rooted-tree variant.
- Implemented PROs use-case in a permissioned blockchain.
- Variants are use-able for experimentation.
- Variants are used in a comparative experiment.
- The experiment is fully reproducible with only a slight variation in results.
- The 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 experiments for the Tendermint Consensus protocol [1].

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

3.7 Required expertise

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

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

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

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

Experiments Knowledge of experimentation within Software Engineering must be gained.

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.

Experimental difficulty Since blockchains are a relatively new subject performance benchmarks and experimental setups may not exist.

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 - Analyze experiment results, write and submit Thesis.

4 Literature survey

Ensuring the proposals' relevance was achieved 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 experimentation 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 the survey and are listed below.

Empirical research on 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.
These contributions should support the pursuance of a Thesis exploring the 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.

[5] Senthil Nathan N. Parth Thakkar and Balaji Viswanathan. Performance benchmarking and optimizing hyperledger fabric blockchain platform. 2018.

Acronyms

Buma Bureau voor Muziek-Auteursrechten. 2

Buma/Stemra Buma Stemra. 2, 5–7

PoC Proof of Concept. 6

PRO Performing Rights Organization. 2–5, 7, 8

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

Stemra Stichting tot Exploitatie van Mechanische Reproduktierechten voor Auteurs. 2

Tx/s Transactions per second. 3

VU Vrije Universiteit. 2