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

April, 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	robertdiebels@grexx.net
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 Summary

The proposed graduate project is part of a larger research project on permission protocols for blockchains. Several parties from the music-industry are interested in this permissioned blockchains as it has the potential to increase efficiency of their businesses. The music-industry's business model is based on payment upon usage of musical works which is enforced by Performing Rights Organizations (PROs). Those who receive this payment should be the rightful owner(s) of the work in question. Fulfillment of this requirement can be accomplished when those who claim ownership are known and if their ownership has been validated. Solutions to this problem often use centralized systems to validate ownership and distribute payment. Those 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. Often these records are duplicated by other PROs as they are unaware of what records their counterparts have.

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 use the music industry's requirements to build a Proof of Concept (PoC) used in a comparative experiment evaluating the capabilities of a permissioned blockchain.

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 Vrije Universiteit (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.

3 Thesis composition

3.1 Problem analysis

In today's society the concept of fundamental ownership of data seems to be neglected. Or otherwise circumvented using "Terms of Use". Data which end-users mark to be deleted does not always get deleted from a system or it may in be stored for years. The proposed project would provide a framework based on blockchain technology giving back ownership of data to its creator or owner.

The identity of artists and their subsequent ownership-claims of created works need to be verified/validated before any payments can take place. This validation is time-consuming some times resulting in payments being delayed for over a year, as collected payments are distributed once a year. Current systems require that humans ensure contracts for usage of works are enforced. It would be preferable to do this instantly upon usage. As such the problem being addressed is one of performance and efficiency.

3.2 Hypothesis

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

Hypothesis Blockchains outperform current ownership-based systems in terms of ownership-validation and usage-permission granting.

3.3 Research method

The proposed Thesis would employ a comparative methodology. The PoC that was built as part of the research project will be used in a comparative experiment. In this experiment it will be compared to current systems and different types of blockchain implementations.

3.4 Research questions

NOTE: Currently most of the research questions below are descriptive and exploratory. Once I have completed the literature survey I will adjust them accordingly.

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 create a PoC using a permissioned blockchain. This PoC will be used in a

comparative experiment in order to gauge permissioned blockchain performance compared to current systems.

3.4.2 Ownership

What types of ownership-validation belong in a permissioned blockchain? Ownership-validation could be extended to digital properties by encrypting them. This would only allow alteration by the property's original creator. A valid question may be which types of ownership-validation belong in a blockchain. Is there a need to document changes to a property?

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 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?

3.4.3 Use-case specific

Interesting questions for the aforementioned use-case would be:

How would the blockchain handle types of permission? For instance how does one define the usages rights of a distribution party like Spotify.

How would the blockchain handle revoking of permissions? Usage rights are defined in contracts. If an artist would want to revoke a contract there would be clauses to deal with such a situation. How would a contract be ended if a clause is deemed illegitimate by a court? How would a contract be ended if the rights were provided until a certain date?

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.

How would a permissioned blockchain handle data-distribution? Parties such as Spotify handle huge amounts of traffic for artists and have the infrastructure to do so. What are the possibilities for blockchains in this area and how would permissions be granted?

How should the permissioned blockchain be optimized? Blockchains can be optimized in a logic to transaction spectrum. The Bitcoin-protocol is optimized for transactions. The Ethereum-protocol is logic-optimized (smart-contracts). Both are unpermissioned chains. How should a permissioned blockchain for this use-case be optimized?

3.5 Expected results

The following list shows the projects' expected results.

- Main: Evaluation of permissioned blockchain capabilities and restrictions.
- Delivered a PoC.
- PoC is an ownership framework, allowing use outside of the music-industry.
- PoC enables further research without too many restrictions.
- PoC is use-able for experimentation.
- PoC is used in comparative experiment.
- Experiment results are used to further evaluate blockchain capabilities.

3.6 Experiment

NOTE: Still need to address comparative experiment. What data will be used in the comparison? How will it be gathered? How does it ensure replication is possible?

3.7 Required expertise

Completing the Master project and the accompanying research the following expertise needs to be acquired.

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 need 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 Thesis. 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 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 Thesis will touch upon those subjects.

3.9 Timeline

- Feb. 22, 2017 - Literature Survey completed.
- Feb. 25, 2017 - Completed changes to Proposal.
- Feb. 28, 2017 - Meeting with SENA, present project proposal.

- Mar. 4, 2017 - Made final adjustments to project proposal and submit to UvA.
- ...

NOTE: Once the survey is done experiment details will be filled in and a precise Timeline can be made.

4 Literature survey

NOTE: Survey still needs to be conducted.