

Master Thesis
- Permissioned blockchains as
ownership-registration systems -

Robert Diebels

As part of a Master graduate project at the Universiteit van Amsterdam

June, 2017

Abstract

Contents

1	Introduction	2
1.1	Bitcoin	2
1.2	Blockchains	2
1.3	Thesis	3
1.4	Contributions	3
2	Literature Survey	4
3	Conclusion	5

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[2] 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 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 may require identification of participants in the real-world. Lowering the chance that there will be malicious nodes active in the blockchain network which requires less validation of transactions, since tampering with records will be less appealing.

1.3 Thesis

Blockchains have a high problem-solving potential [1] though the technology is still lacking in certain areas [3] [4]. Permissioned blockchains in particular have not received much attention concerning comparison with current market systems they can replace.

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 evaluated based on throughput compared to one another and the in-use systems.

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

Chapter 3

Conclusion

Bibliography

- [1] Juri Mattila et al. The blockchain phenomenon—the disruptive potential of distributed consensus architectures. Technical report, The Research Institute of the Finnish Economy, 2016.
- [2] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
- [3] 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.
- [4] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, and Huaimin Wang. Blockchain challenges and opportunities: A survey. 2016.