Literature Survey - Ownership using Persmissioned Blockchains

Robert Diebels

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

May, 2017

Abstract

Blockchain-technology is a technology which allows retaining of trust between transaction parties without an intermediate party. Blockchains achieve this by ensuring all of the parties partaking in the blockchain keep a copy of all transactions undertaken so far. By ensuring all parties keep a copy of transactions parties are able to verify the correctness of new transactions.

Blockchains which restrict access to the blockchain are called permissioned blockchains. How these blockchains restrict access depends on the purpose of the blockchain. For instance, it could be a requirement that a participant has been verified to be a certain person. Where other implementations simply require an email-address.

This literature survey aims to (1) evaluate the current state of scientific literature on permissioned blockchains, (2) evaluate current implementations of permissioned blockchains, (3) evaluate the state of experimentation on permissioned blockchains, (4) collect research on blockchains for the music-industry. This is done with the purpose of supporting a Master graduate project on using permissioned blockchains in the music-industry.

The results of the survey show 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.

Index terms— blockchain, permissioned blockchain, survey, review, thesis, music-industry

1 Introduction

Society is increasingly digitizing many previously physical assets. As with physical assets these digital assets have owners, are sold and bought on a regular basis. With the rise of technology such as Bitcoin [2] attention is being given to similar technology applicable to a wider range of digital assets.

In 2008 [2] introduced an electronic payment system based on cryptographic proof called Bitcoin. The motivation to develop Bitcoin was to eliminate the need for financial institutions which act as a middle-man responsible for validating and verifying transactions. Bitcoin's design combines several technologies which allow it to ensure currency transactions are validated and verified without an intermediate party. Underlying Bitcoin is a peer-to-peer network. In this network each node keeps a record of all previously enacted transactions. Keeping a local copy of transactions allows a node to independently verify correctness of new transactions. Removing the need for a middle-man.

Each new node in the network gets a public-private key pair which is used to sign transactions the node performs. Signing a transaction provides verifiability of ownership and has the benefit of not disclosing the identity of anyone who is using the node.

New transactions that have been validated are grouped into blocks in a process called mining. Blocks are linked to previously created blocks to create a chain. The principle of grouping transactions into blocks and linking blocks gives blockchain-technology its name.

Mining involves grouping transactions into blocks and hashing the block twice using SHA-256 until the hash is smaller than a given target value. If a block is found that yields the target value it cannot be changed without redoing the work done to identify it. The block is then submitted for validation, if valid it is broadcast onto the network.

Permissioned blockchains are a type of blockchain which contrary to Bitcoin have access control in place. Limiting which nodes are allowed to submit transactions, verify transaction and depending on the protocol used which nodes can form blocks.

This survey aims to evaluate current scientific literature on permissioned blockchains and the state of permissioned blockchain implementations. This is achieved by performing a mapping study as defined by [4]. This survey deviates on the approach defined by [4] on some points. The surveys' deviations, scope-definition and data-extraction items can be found in section 2. The extracted data-items defined in section 2 are used in sections section 3 and section 4 illustrating several key facets of the selected articles and implementations. Section 5 discusses the surveys results based on the defined research questions. The survey ends with section 6 in which the surveys' conclusions are reported.

2 Approach

This survey builds on a systematic mapping study as defined by [4] and implemented by [5]. The modification was done to limit the time spent on the survey. The process as defined by [4] is as follows:

1. Formulate research questions to determine the scope of the survey.
2. Conduct a search collecting scope related articles.
3. Screen the collected articles based on relevancy.
4. Collect keywords from the relevant articles' abstracts to create a classification scheme.
5. Extract the necessary data in order to create a systematic map.

The survey deviates from this approach as it is undertaken as part of a Software Engineering (SE) graduate project. With the goal of evaluating the current body of work on permissioned blockchains. Certain data need not be extracted from the selected articles to serve that purpose.

Further deviation arises as a result of the surveys' scope definition. RQ2 requires a search to be performed to locate current implementations of permissioned blockchains. Both [4] and [5] do not define a process to gather literature or information on implementations of a technology. Ensuring data on implementations was gathered in a structured manner the process defined by [4] was adapted to include both implementations and literature.

2.1 Scope definition

As part of the approach the following research questions were defined to limit the scope of the survey.

RQ1 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.

RQ2 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.

RQ3 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.

RQ4 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.

2.2 Search results

Based on the defined scope a set of search terms for articles and implementations was defined.

Articles Article search terms were entered into Google Scholar and the Universiteit van Amsterdam (UvA)'s online library. An overview of the defined search terms and the results yielded can be found in Table 3.

Matching The search was performed using on exact search term matching. Meaning the terms should yield results matching the order in which keywords are entered. When a search yielded no results with exact matching default matching on keywords was done. A drawback of default matching is that it yields more results as there are no limitations on order. Which can misrepresent the amount of research done on a topic.

Exclusion Search results excluded books, patents and citations. Books were excluded due to time-constraints on graduate project completion. Patents and citations were excluded giving a more realistic view on the amount research done.

Implementations The implementations search was conducted by searching on Google. A clear set of search terms was not defined and most implementations were gather by reference from technical blogs and/or webinars.

Inclusion Implementations were included if they fit the music-industry's use-case or were adjusted-able to accommodate it.

2.3 Search result screening

Selection of relevant literature was done by filtering based on title and reading an articles' abstract. Part of the literature came from fields unrelated to SE. They contain evaluations of permissioned blockchains which were deemed useful. In particular analyses of adoption rates were added to the selection as they provide insights concerning current usage constraints.

Inclusion: All inclusion criteria during screening are listed below and were checked for each article in the order in which they are listed.

1. Title similarity to defined scope.
2. Language, English or Dutch.
3. Similarity of field to SE.
4. Abstract screening.
5. Skimming [1].

Once the screening process was finished the amount of included articles was 25. Screening results per criteria can be found in Table 4.

[1] Skimming was done when field similarity to SE was low yet the abstract revealed interesting insights. This ensured that articles were relevant for the graduate project.

2.4 Keyword collection

Collection of keywords from articles was done by following a similar process as [5, p.6] and [4, p.3-5]. This was done by (1) reading the abstract and identified keywords, (2) clustering keywords into categories, (3) reading the selected articles, (4) checking references and possibly adding referenced to the selection.

This survey deviates from the approach of [5] and [4] by allowing referenced articles to be added to the article selection during keyword collection.

2.5 Data extraction

During the key-wording and screening process a number of data extraction items for were decided upon. Items were selected based on relevancy to the surveys' scope and importance to the screening process.

Articles A full list of data extraction items for articles can be found in Table 1.

Implementations Data extraction items for implementations can be found in Table 2.

ID	Data item	Description
DIA01	Title	Title of the article.
DIA02	Year	Publication year of the article.
DIA03	Contribution keywords	Contribution keywords extracted during key-wording.
DIA04	Context keywords	Contextual keywords extracted during key-wording.
DIA05	Blockchain type	Which type of blockchain the article addressed: permissioned, permissionless or both.
DIA06	Research facet	The type of research done [4, p.4].
DIA07	Contribution facet	What type of contribution the article had in respect to blockchain-technology.
DIA08	Experiment facet	Articles with contribution facet 'Application' or 'Improvement' or research facet 'Solution Proposal' the were checked for experiments and experiment purpose.

Table 1: Article data extraction items and their description.

ID	Data item	Description
DII01	Name	Name of the implementations.
DII02	Year	Release year of the implementation.
DII03	Located year at	Short description how the release year was determined.
DII04	Homepage	Implementation's homepage.
DII04	Type	What the type of implementation is.
DII05	White-paper/proposal	Location of the original white-paper or proposal. (URL)
DII06	Yellow-paper	Location of the original yellow-paper. (URL)
DII07	Permissioning	Does the implementation allow for permissioning of the ledger?
DII08	Located permissioning at	Where it is stated the ledger allows permissioning.
DII09	Consensus protocol	The name of the consensus protocol.
DII10	Consensus Repository	Location of the consensus protocol's repository. (URL)
DII11	Open-sourced	Has the implementation been open-sourced? (Yes/No)
DII12	Repository	The code repository of the implementations. (URL)

Table 2: Implementations data extraction items and their description.

3 Basic information

This section contains an overview of basic information of selected articles and blockchain implementations. Search and selection results are shown where applicable.

3.1 Articles

Data-extraction items DIA01 and DIA02, title and publication year respectively, were used to determine article basic information.

Search and selection After a scoped search was conducted and all inclusion criteria were applied a total of 25 articles remained. Of which 1 reported on blockchain applications within the music-industry. All search term results are show in Table 3. Results per selection criteria are shown in Table 4.

Search term	**Google scholar**	**UvA's online library**
permissioned blockchain	81	17
permissioned blockchains	92	17
private blockchain	124	189
private blockchains	127	53
blockchain survey*	2,060	55
blockchain review*	4,360	86
permissioned blockchain survey*	91	2
permissioned blockchain review*	163	1
private blockchain survey*	1,590	23
private blockchain review*	2,340	46
music industry blockchain*	951	31
music-industry blockchain*	111	13
Total (including duplicates)	12,090	533

Table 3: Articles found by search term
*: Search terms which yielded 0 to 5 results for exact matching.

Inclusion criteria	**Remaining articles**
Search results	12,090/533
Title	31
Language	31
Similarity to SE	30
Abstract screening	29
Content skim	25

Table 4: Remaining articles after inclusion criteria application.

Publication year Figure 1 shows the amount of articles published per year.

It is worth noting that out of 25 selected articles a total of 19 articles was published in 2016, showing an increase in blockchain research. This agrees with the trend noted by [5] which was published in 2016. Where it was found that most research was published in 2015 indicating an increase of blockchain research publications. This would indicate that the amount of blockchain research publications is still increasing.

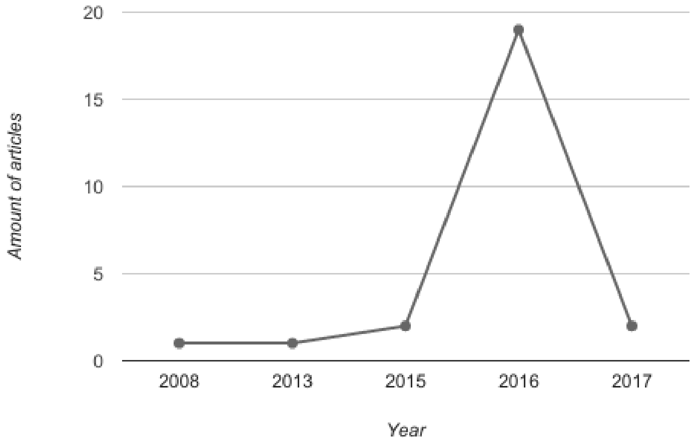

Figure 1: Published articles per year

3.2 Implementations

The following data extraction items were used to determine basic information of implementations: DII01, DII02 and DII04. Representing name, year and type.

Search and selection During the search and selection process a total of 12 blockchain-like implementations was found.

Release year Figure 2 shows the amount of blockchain-like implementations. The figure shows that along with increasing research interest in 2016 the amount of blockchain-like implementations increased significantly in the same year.

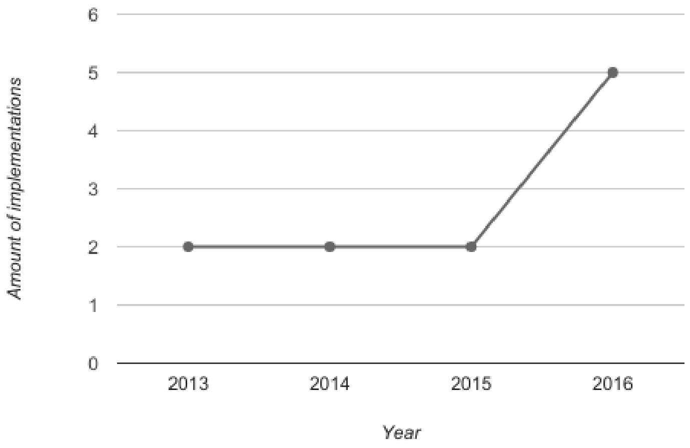

Figure 2: Released implementations per year

4 Classification

This section serves as a classification of selected articles and implementations.

4.1 Articles

Classification of articles was based on data extraction items DIA05-DIA08.

Blockchain facet Determining which type of blockchain an article targets assures that article inclusion criteria were correct. After data-extraction was performed a total it was revealed that of the 25 examined articles 15 articles targeted permissioned blockchains and 9 targeted both permissioned and permissionless blockchains. Only 1 article targeted permissionless blockchains. Serving as an indicator that the inclusion criteria sufficed in ensuring articles addressing permissionless blockchain were excluded from the selected articles.

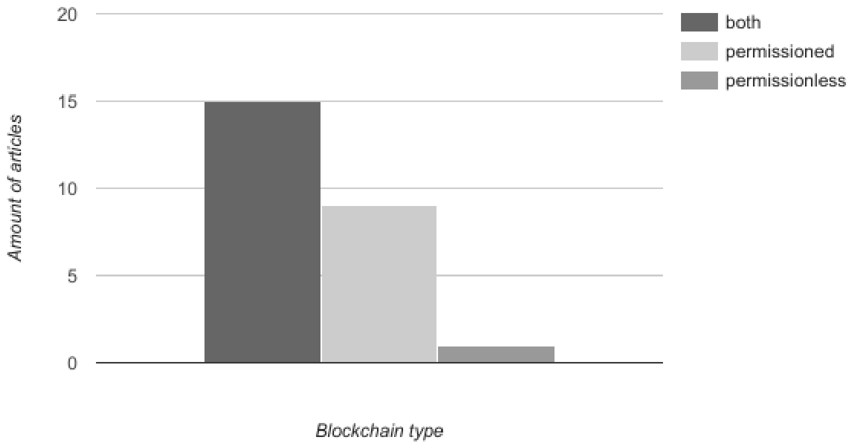

Figure 3: Researched blockchain types

Contribution facet Figure 4 shows the classification of articles by the type of contribution they made. Out of 25 articles 12 suggested improvements and provided an application of blockchain-technology. Articles classified as reports on the state of blockchain-technology amounted to a total of 7. All other classifications had either 1 or 2 articles in total.

This suggests that research done in the field is focused on improving current flaws and exploring the state of blockchain-technology. As most articles provide improvements and applying them as a suggested solution.

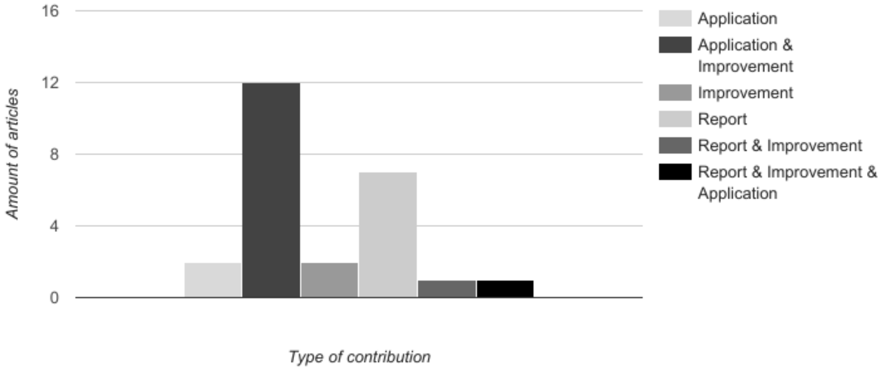

Figure 4: Research contribution types

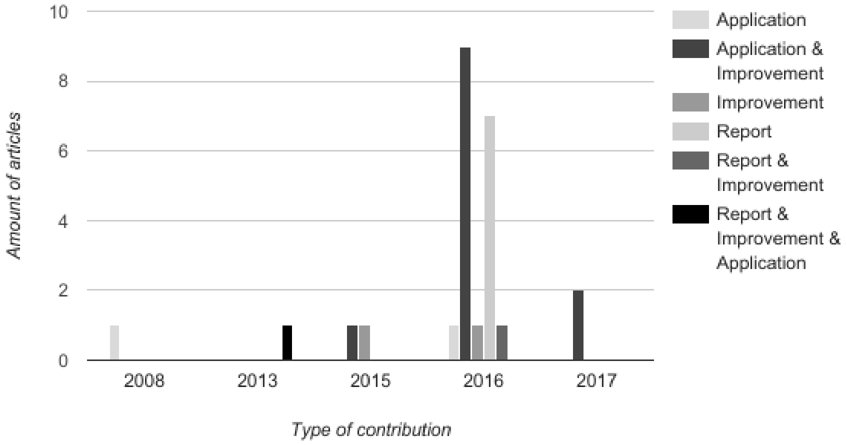

Figure 5: Researched blockchain types per year

Experiment facet Classifying articles in terms of experimentation was done to examine the state of empirical evidence gathering. Classification was performed on articles that were classified as providing a contribution of all types excluding reports. The final classification as shown in Figure 6 reveals that out of the 16 papers included 56% performed no experimentation. Another 7 articles or about 43% performed experimentation to validate an application of blockchain-technology.

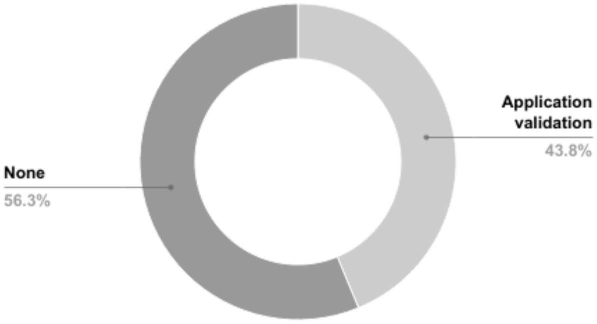

Figure 6: Performed experiment types

Topic facet Using the contribution and context keywords gathered for each article a set of topics was defined. The set was grouped into 3 categories (1) topics about permissioned blockchains, (2) topics on improving blockchain flaws, (3) other topics relevant to the field.

1. Permissioned blockchains
   (a) Access control
   (b) Identity management
   (c) Immutability
2. Blockchain improvements
   (a) Smart-contracts
   (b) Consensus protocol
   (c) Privacy preservation
   (d) Anonymity
3. Other topics
   (a) Internet of Things
   (b) Adoption rate
   (c) Anti-money laundering

4.2 Implementations

Classification of implementations was done based on data-extraction items DII04, DII07 and DII11. Respectively type, permissioning and open-sourced.

Implementation type Figure 7 shows that out of the 12 implementations that were classified 7 were blockchains implementations. Another 2 implementations were related to blockchains in the sense that they use distributed ledgers. Upon inspection it was revealed that the remaining 3 implementations had more in common with payment-systems connecting ledgers than blockchain implementations.

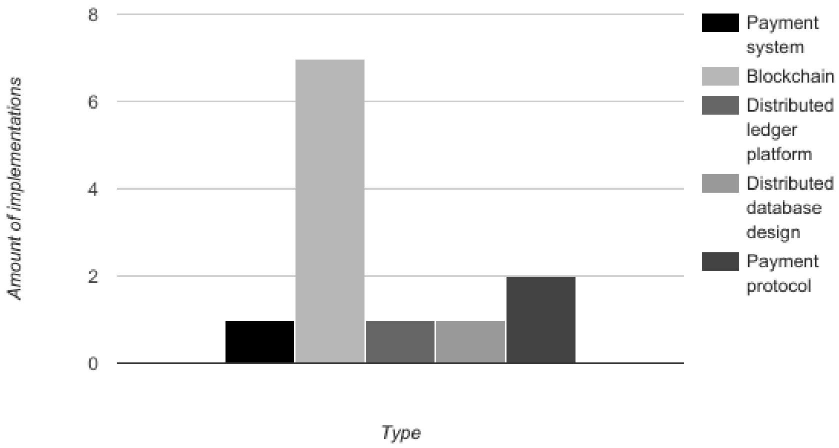

Figure 7: Implementation types

Permissioning Out of the 12 found 8 implementations have the possibility to enable permissioning or are permissioned by default.

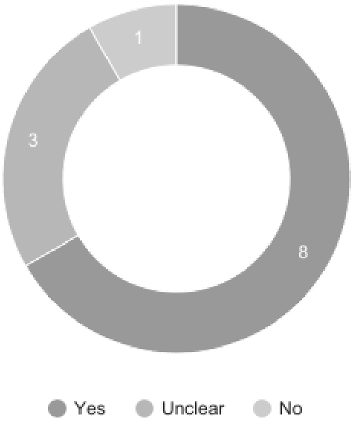

Figure 8: Permissioning allowed

Open-source All of the included implementations have open-sourced their code. It has not been investigated why this was done as it was not within the scope of this survey.

5 Discussion

This section goes through the search results and their subsequent classification answering the four research questions defined in subsection 2.1.

5.1 RQ1 – Which topics are addressed in current research on permissioned blockchains?

Categorizing the keywords of selected articles revealed a set of topics relating to permissioned blockchains. The topics concerned access-control, identity-management and immutability of the blockchain.

Other topics concerned improvements to blockchain flaws such as smart-contracts, consensus protocols, privacy-preservation, anonymity guarantees and application related research in, for example, the Internet of things.

5.2 RQ2 – What implementations of permissioned blockchains exist?

Search results revealed that there are 8 implementations with permissioning of which 5 were blockchains.

Another 2 implementations had blockchain-like properties such as a consensus protocol and distribution of transactions across a network. This addresses the flaws blockchains have in terms of throughput and latency. By replacing consensus protocols with other systems higher throughput is achieved. In turn other properties of the blockchain are sacrificed such as its decentralized nature.

5.3 RQ3 – What experiments are being performed on permissioned blockchains?

Evaluation of experimentation in current scientific literature revealed that out of the 16 articles included in the evaluation 7 articles contained a defined experiment. All of which were done in other to validate a proposed solution to improve blockchains.

None of these articles were aimed at reproducing findings of other studies or comparing current implementations of permissioned blockchains.

5.4 RQ4 – Is there any research on blockchains related to the music-industry?

Out the 25 found only 1 was directly related to the music-industry. In the report [3] 4 potential uses of blockchains are provided: (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.

The first potential benefit is directly related to the use-case the graduate project seeks to explore. Which appears to confirm the potential of using blockchains in a music-industry setting.

Research on blockchain usage in the music-industry was not found. Indicates that the graduate project can make a significant contribution to the field.

6 Conclusions

Aside from its use in cryptocurrencies blockchain-technology has a wide range of potentially useful applications. Permissioned blockchains specifically could be used to build systems in which access control needs to be enforced.

This survey set out to identify current research topics on permissioned blockchains, the state of experimentation on permissioned blockchains in scientific literature, which implementations of permissioned blockchains exist and assessing whether any research on the use of blockchains in the music-industry has been published.

To accomplish this a mapping study was performed and structured in a similar way to [4]. Adjustments to that process were made to accommodate inclusion of implementations rather than literature.

A total of 25 articles and a total of 12 implementations were evaluated and classified. The evaluation led to the following conclusions.

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] [6].

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.

References

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

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

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

[5] 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.

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