University POLITEHNICA of Bucharest

Faculty of Automatic Control and Computers,
Computer Science and Engineering Department

BACHELOR THESIS

Exploring Decentralized Name Services using Namecoin

Scientific Adviser:
Prof. Magnificus Academicus

Author:
Adriana Dinca

Bucharest, 2017

Maecenas elementum venenatis dui, sit amet vehicula ipsum molestie vitae. Sed porttitor urna vel ipsum tincidunt venenatis. Aenean adipiscing porttitor nibh a ultricies. Curabitur vehicula semper lacus a rutrum.

Quisque ac feugiat libero. Fusce dui tortor, luctus a convallis sed, lacinia sed ligula. Integer arcu metus, lacinia vitae posuere ut, tempor ut ante.

Abstract

[LM: General abstract idea: (see https://github.com/spyked/scribblings/blob/master/misc-notes/sfaturi-redactare-lucrare.markdown):

- **Localize: we want naming and identity systems that are decentralized, secure, human-readable (Zooko's triangle problem); traditional solutions (DNS, Tor services, etc.) do not provide all these properties; fortunately Namecoin, a solution based on the Bitcoin blockchain, is a promising solution.**
- **Focus: Namecoin is a new system; although it has gathered some popularity in the scientific community, documentation is sparse, we don't know how it has been used until now, and we lack information on the possibility of storing specific types of information (e.g. certificates for authentication) on the blockchain.**
- **Report: We aim to fill this gap of knowledge; to study the protocol, we propose a new tool, Namecoin Explorer, that allows browsing, aggregating ... [fill in] naming information in the Namecoin blockchain;**
- **Argue: We implemented a prototype of Namecoin Explorer; we evaluated it by gathering data from the Namecoin blockchain; our evaluation shows that ... [highlight important findings].**

]

Naming and identity services is a widely used concept implemented in multiple technologies. These systems should have three basic attributes: secure, descentralized and human-readable. The most used naming systems are DNS, Tor services and OpenID. DNS is both secure and human-readable by using a mapping between network addresses and domain names. Tor services are used for anonymous communication. Tor aims to remove trace between user's identity and his online activity but there is no guarantee for anonymity. OpenID protocol allows us to use an account to sign in to multiple websites without having a username and a password for each website. Although, these technologies perform well, none of them provide all three properties. The traditional naming system involves trusting a third party. The Namecoin protocol resolves the trust issue by using a distributed network of Bitcoin blockchain nodes for validation operations. The Namecoin claims to gather all three properties but the protocol's documentation is sparse and there is a lack of information on the possibility of storing specific types of data(e.g. cerificaticates for authentication) on the blockchain. The Namecoin technology is quite young and unexplored enough so we aim to create an exploring solution.

There is no tool available for discovering Namecoin's naming services so we build a prototype for exploring the Namecoin's domain name specifications. As a result of our exploration, we validate protocol technical implementation details. Our evaluation outlines that a small group of stackholders has the majority of Namecoin domain names so the Namecoin network is less trustworthy.

[LM: Avoid colloquial expressions, e.g. “what’s so interesting about x”, “was worth it”, etc. Try to remain objective when building the argument.]

Contents

List of Figures

List of Tables

Chapter 1

Introduction

[LM: The purpose of the introduction is to provide some details about the thesis: context, problem statement/motivation, solution summary and evaluation summary. Basically it's a more elaborate restatement of the abstract. My proposal—to be reviewed by everyone :)—is to use the following structure:

- **a problem overview and very short (a couple of sentences) description of the thesis**
- **a "thesis goals" subsection describing the goals in paragraphs**
- **a "summary" subsection summarizing (one sentence each) the thesis chapters**

Related work should be part of the background section. I don't think we need a related work per se, although you could describe in short other blockchain explorers and discuss why they are insufficient for what we needed.]

1.1 Project Description

1.1.1 Project Scope

The main scope of this project is to qualify Bitcoin [1] for use in critical systems **[LM: I think the scope is a bit too broad; in principle, we want to explore decentralized naming systems, etc., in particular Namecoin]**.

[LM: Review https://github.com/spyked/scribblings/blob/master/misc-notes/sfaturi-redactare-lucrare.markdown for guidelines on how/what to cite (ask if in doubt).]

Although, the Bitcoin project is the most popular blockchain based application there are other blockchain projects that deserves to be brought to attention such as Ethereum, Namecoin or Ripple. The Ripple project started before Bitcoin in 2004 and it passed through many changes over time. Today, Ripple is a solution that enables banks and clients to exchange value. Similar with Bitcoin, Ripple is a distributed system with its own blockchain and a native currency called ripples. Ethereum is another blockchain based application that has its own Turing-complete programming language which makes it more powerful than Bitcoin by allowing users to create their applications on any programming language. Namecoin was the first fork of the Bitcoin project. It offers a domain name registry similar to the Internet's DNS. It is an alternative domain name service for the root domain .bit. The project has its own currency called namecoins (symbol NMC), which is used to pay transactions fee for registration, update and transfer of domains name.

1.1.2 Project Objectives

1.1.3 Related Work

The Bitcoin invention is a story of evolution. It is the evolution of electronic cash, payment systems, how money are transferred over the world and even how the business looks nowadays. Prior Bitcoin, electronic cash and digital currencies were available only in centralized systems. An example would be the SWIFT protocol that enables financial and non-financial institutions to transfer financial information via ISO standardized messages.

What's so interesting about Bitcoin technology is how it solves both the problem of double-spending and mining in a decentralized system. The protocol is developed on "sound cryptographic" principles that guarantees proof-of-work, proof-of-ownership and classic currencies attributes such as fungibility and scarcity.

The Bitcoin project introduces proof-of-work for mining and a consensus protocol based on Byzantine Generals' Problem to eliminate double spending. More than that the protocol uses a blockchain structure for storing data. Satoshi Nakamoto, the Bitcoin's creator describes the solution to the Byzantine Generals' Problem and how it can be implemented for achieving consensus on the Bitcoin distributed network in a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" .

What draw our attention to the Namecoin protocol is the fact that it is quite a young project and it will be interesting to understand how is it used and how the data is stored in the blockchain. There is no systematic documentation of the protocol so by writing a report that organize Namecoin specific information we want to make our contribution to this project. In addition, we started working on a tool that explores the Namecoin blockchain and validates the statements of this report.

1.1.4 Demo listings

1.1.5 Tables

Chapter 2

Background

2.1 Background

2.1.1 Overview

The use of electronic cash is indisputable one of the greatest benefits of the modern world. This wouldn't be possible without the existence of a mechanism that ensures the use of a common language for financial message exchange. As a result, the Society for Worldwide Interbank Financial Telecommunication was born. SWIFT network has standardized messages for financial information transfer. Some examples of ISO standards used for transfer of electronic cash are ISO 15022 MT and ISO 20022 MX. Although the advantages of using digital currencies are obvious, the main disadvantage is the fact that these systems are centralized. Satoshi Nakamoto is the creator of the first distributed system used for financial transfer by introducing the Bitcoin protocol. Based on prior work, Bitcoin introduces proof-of-work for cash minting, uses the blockchain for data storing and a consensus protocol based on the Byzantine Generals' Problem to eliminate double-spending.

2.1.2 Proof-of-work system

The idea of using a proof-of-work system to legitimate the user of an application was used before in other software systems. For example, hashcash is a proof-of-work system introduced by Adam Black in 1997 that was invented to limit email spam and denial-of-service attacks. The idea is quite easy to follow: a legitimate sender needs to spend a reasonable amount of computing time in order to send an email. If a legitimate user sends a reasonable number of emails, a spammer wants to send thousands of emails making the spamming effort very expensive. The receiver's role is to validate the hash, which is quite easy. Hashcash is conceptually similar to the proof-of-work system used by Bitcoin miners.

2.1.3 The blockchain

What's so innovative about the Bitcoin protocol is that it brings together users with wallets containing keys, miners who collect transactions and add them to the blockchain and transactions that are propagated across the network.

The blockchain is a public ledger of all transaction sent through the network that is known by every one that holds a Bitcoin/Namecoin node. More precisely, each node has a copy of the blockchain in order to validate or invalidate a transaction. The majority of nodes decide if a transaction is valid and if so that transaction is added in the latest created block by one of the miners. The choice of using blockchain for data storing is related with the fact that the blockchain's deep history is immutable so it ensures the Bitcoin security.

The blockchain is a peer-to-peer system with no central authority that has the role of managing bitcoin flow along the bitcoin nodes network. This technology is recognized as the "fifth evolution" of computing, the missing trust interface of the Internet.

It contains three important parts: the block, the chain and the network. The block is an array of transactions recorded into a ledger. Depending on the blockchain the transaction has assigned a different type of value. Each block has its own hash and a merkle tree with hashed transactions. Storing transactions in a merkle tree is a design decision that saves disk space. Satoshi Nakamoto explains the reason why using a merkle tree makes disk space recover possible in his paper, "Bitcoin: A Peer-to-Peer Electronic Cash System". The explanation for this is that "Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree, with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored".

The chain is simply a hash that connects two blocks in chronological order. The hash for a new block is generated based on the data that was in the previous block. The hash algorithm used by Bitcoin is Secure Hash Algorithm 256 that creates an unique (collision probability is negligible), fixed-size (256 bits) hash.

The last key component, the network is represented by full nodes. We can think of it as a computer that runs an algorithm for securing the network. Mining is expensive and it requires a lot of computer power so the blockchain algorithm rewards miners for their service. The payment is usually a currency or a token.

2.1.4 Naming and identity system

Namecoin project is based on the Bitcoin protocol and it solves issues such as naming and identity in a distributed system. What's more about Namecoin that made us want to explore and discover the protocol specific details is the fact that this protocol is new, there is a lot of data that is stored in the blockchain that was not explored yet and in addition this protocol was able to solve a computer science problem called the Zooko's triangle Problem.

Zooko's triangle represents the fact that a naming system is able to achieve only two of the three desirable attributes: human meaningful, secure and decentralized. The idea of placing these three attributes in a corner of a triangle can be described as follows. In a triangle only two corners can be connected by a single line so the three attributes will never be connected by the same line when placed in corners just like a system that couldn't focus on all attributes.

For example, OpenID which is a identity protocol that allows us to carry our identity across other websites without the need to register again focus only on security and human meaningful. The decentralized aspect is not solved so we have to trust at least one service provider. This protocol is used by companies like Google, Yahoo!, Twitter.

To solve the Zooko's triangle problem, the Namecoin protocol was developed and until now there is no other protocol that was able to focus on the three attributes. The Namecoin is a third-party identity provider, the blockchain, that can be used as an intermediate step between someone (maybe a service) that wants to know your identity and you. Until 2011, the design of a system that follows the Zooko's triangle was impossible. In order to have a namespace system that is secure and easy to work with, a user should be able to choose namespace strings that mapped with a certain value are uniquely identifying a network node and that no one can convince a node that other value for that pair is correct.

Although, the Namecoin system is not free of security attacks and errors this is the first system that solved the Zooko' s triangle by using cryptocurrency technology. This protocol is limited to the human-legible phrases but has the advantage of making a name choice. More than that, the namecoin is the first alt-coin developed by forking the Bitcoin project. Namecoin implements both a merged mining and a decentralized DNS.

Building a system that is decentralized based on the Bitcoin project was done by creating another blockchain using a new genesis block. This system has also several specific transaction types in order to provide a domain name system features. The only TLD used is .bit.

2.1.5 Namecoin

[LM: I created a new macro for defining pieces of code. For example: `name_new` should typeset function names more easily.]

[LM: Some diagrams would work great here. What we're particularly interested in:

- **how the protocol works, overlaid on top of blockchain technology – how a domain name is registered, how it is expired, how it is validated (using the blockchain), how it is resolved. Basically this should answer the question "how does Namecoin solve Zooko's triangle problem?".**
- **how the interaction with Namecoin goes on the user side – the blockchain is downloaded locally, the user communicates with a Namecoin node through a browser plugin, etc.**

This is in my opinion *very* valuable, and although it's not part of our contributions, it is something that we *found out* in our exploration.]

The Namecoin transaction types used for identifier registration are the following: name_new, name_firstupdate and name _update. In order to make a request to register a new domain the name_new transaction is called using the syntax 'name_new identifier'. The transaction name_firstupdate is used for adding information in the value field of a transaction. This field has no fixed structure and everyone can add different type of data such as digital certificates, files, contact information and so on. This transaction type must be done 12 blocks after the new_name transaction was generated and it is called only once for a certain domain. The syntax is 'name_firstupdate identifier rand tx value'. The last type of Namecoin transaction is the new_update that is used for updating the value field, for changing the ownership or for renewing the domain. It is called using the following syntax: 'name_update identifier value toaddress'.

There are also Namecoin transactions that meet other purposes such as identifier lookup (name_filter, name_history, name_list, name_scan and name_show), namespace specific (domain_show and identity_show), maintenance (name_clean), general commands for controlling (getinfo, help, stop) and network commands (addnode, getaddednodeinfo, getconnectioncount, getnettotals, getpeerinfo, ping). The Namecoin protocol has also support for Bitcoin specific transactions related with blockchain, mining or wallet.

Namecoin uses an identity system based on addresses. Namecoin addresses are Base58 encoded hashes of receivers' public keys. All payments and records are made to addresses. Namecoin records have a key and a value with the following syntax. The key namespace/name identify the website name.bit. The value should match the DNS namespace specification. In order to register key-value pair the user has to spend namecoins. Once the user owns their key-value pair the value field is available for 35999 blocks. After reaching this number the value will expire and you need to spend Namecoins to update it. For the key field there is no expiration condition. Another Namecoin protocol specification is the possibility to organize different types of keys. There are some popular namespaces such as a (application specific data), d (domain name specifications), ds (secure domain name), id (identity), is (secure identity) and so on. In addition, everyone can create new namespaces or organize his/her keys based on already existing namespaces. Some examples of domain name specific information that are stored in the blockchain:

```
{
"name": "d/nf",
"value": "{\"map\":{\"\":\"94.23.252.190\"}, \"fingerprint\":
[\"69:16:99:8B:A7:62:6F:BE:2A:F6:AF:62:E4:DA:4D:8F:32:B8:52:28\"]}",
"expires_in": 34458
}
{
"name": "d/nh",
"value": "{\"for_sale\" : 1, \"website\" : \"http://blockchained.com\",
\"name\" : \"phelix\"}",
"expires_in": 34921
}
```

Chapter 3

Design

3.1 Project Design

3.1.1 Project Design Brief

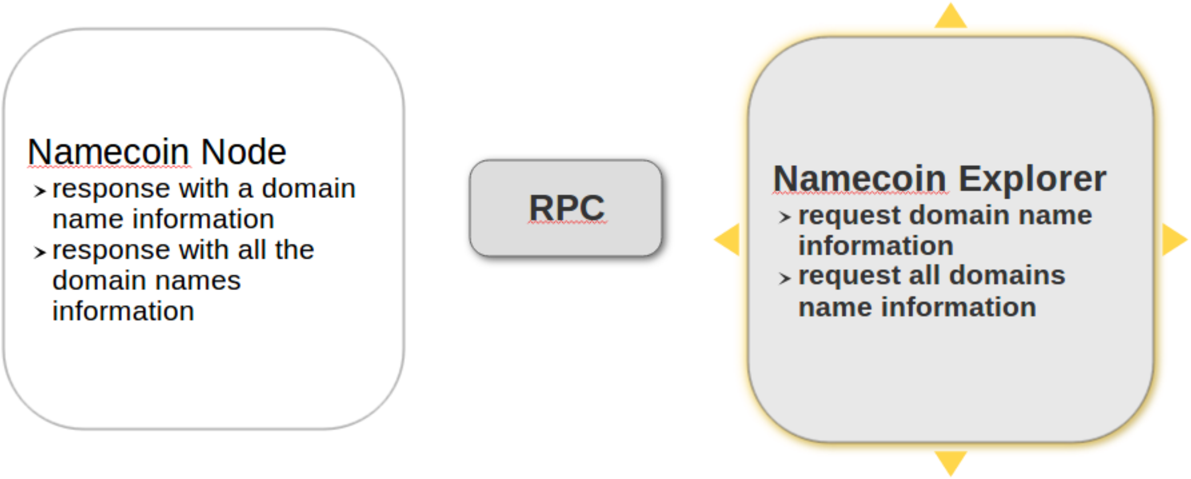
Namecoin Node
› response with a domain name information
› response with all the domain names information
RPC
Namecoin Explorer
› request domain name information
› request all domains name information

Figure 3.1: Design Namecoin Explorer

We propose an exploration tool for Namecoin, that allows the user to obtain all relevant information about a certain register identity transaction type and that help Namecoin node owners to discover, validate or explore information stored in the blockchain. For example, this type of information may be of interest of a user who wants to buy a domain that is already owned by somebody else.

The idea is to create an application that connects to a Namecoin node and to get the relevant data based on the type of the request sent. The Namecoin project offers an API to ask for some specific information about DNS records using RPC mechanism. The Namecoin node has the server role providing data from blockchain to a client. The client is a Java application that displays both information for a .bit domain or for all .bit registered domains.

Chapter 4

Current Status

4.1 Current Status

4.1.1 Current Status Brief

At this point, most of the research work was done, followed by the design and in the end the implementation of our explorer application. The last step of our strategy is in a beginner stage but we are confident that all the time allocated to namecoin client analysis is in our favor by building an application that gathers as much information as possible and that is also useful to different clients.

Chapter 5

Summary and Future Work

5.1 Summary and Future Work

5.1.1 Summary and Future Work Brief

This paper tries to put together all the knowledge acquired and to organize it in a logical order, making a contribution to everyone new to Namecoin, with no background in the Bitcoin field. From the very beginning this paper presents the fundamental principles of Namecoin by describing the Bitcoin features that are used in the Namecoin and other specific information that make Namecoin protocol so interesting. The Namecoin is quite new and there are a lot of information which might be of interest both for Namecoin users or for somebody new to this technology.

Appendix A

Project Build System Makefiles

A.1 Makefile.test

```
# Makefile containing targets specific to testing

TEST_CASE_SPEC_FILE=full_test_spec.odt
API_COVERAGE_FILE=api_coverage.csv
REQUIREMENTS_COVERAGE_FILE=requirements_coverage.csv
TEST_REPORT_FILE=test_report.odt


# Test Case Specification targets

.PHONY: full_spec
full_spec: $(TEST_CASE_SPEC_FILE)
        @echo
        @echo "Generated␣full␣Test␣Case␣Specification␣into␣\"$^\""
        @echo "Please␣remove␣manually␣the␣generated␣file."

.PHONY: $(TEST_CASE_SPEC_FILE)
$(TEST_CASE_SPEC_FILE):
        $(TEST_ROOT)/common/tools/generate_all_spec.py --format=odt
            -o $@ $(TEST_ROOT)/functional-tests $(TEST_ROOT)/
            performance-tests $(TEST_ROOT)/robustness-tests
#

# ...
```

Listing A.1: Testing Targets Makefile (Makefile.test)

Bibliography

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *The Cryptography Mailing list at metzdowd.com*, 2008.