Namecoin

Andreas Loibl
Betreuer: Johannes Naab
Seminar Innovative Internettechnologien und Mobilkommunikation SS2014
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: andreas.loibl@tum.de

ABSTRACT
This paper gives a brief introduction into alternative naming systems and how they can prevent and circumvent censorship. It explains the concepts of the peer-to-peer (P2P) based cryptocurrency Bitcoin and how it can be extended to implement an alternative naming system (Namecoin) without a need for a trusted authority. Namecoin domains are stored in the distributed Namecoin blockchain, a public ledger of every Namecoin transaction ever executed. It does not integrate directly in the regular domain name system (DNS), in order to resolve such domains a browser addon/extension is required. Problems like this lack of integration and usability have prevented Namecoin from being widely used currently.

Keywords
Namecoin, Bitcoin, DNS, NMC, BTC

1. INTRODUCTION
Within the current DNS structure the server operators have the power to censor information by seizing or redirecting domain names. For example, in the weeks before the local elections the Turkish government blocked Twitter and Youtube by redirecting their DNS records [1]. Another example is China, where DNS cache poisoning is commonly used to censor domains for their citizens [2].

One possible way to prevent and circumvent censorship like this is Namecoin, a distributed, secure and trustless domain name system that has no central authority.

In section 2 the paper presents the properties of naming systems and cryptocurrencies. Section 3 gives an introduction to Namecoin and explains how to register domains within the Namecoin namespace, what those domains can be used for and compare this system to regular DNS and other alternative naming systems. The paper concludes with section 4 after outlining problems and usage statistics of the current Namecoin implementation and in section 5 the referenced materials are listed.

2. ZOOKO'S TRIANGLE
Zooko Wilcox-O'Hearn [3] claims that any naming system can only fulfill two of the following three desirable properties:

1. Secure, i.e. globally unique: There is only one, unique and specific entity to which the name maps. Nobody can successfully pretend to be the owner of someone else's domain name.
2. Decentralized: There is no centralized authority for determining the meaning of a name.
3. Human-meaningful: Names are arbitrarily chosen strings short enough for humans to memorize.

This leaves three possible choices to implement a naming system [4]:

- Compromise decentralization: e.g. DNSSEC is secure and human-meaningful, but not decentralized. It is implemented with digitally signed records for DNS lookups using public-key cryptography.
- Compromise human-readability: e.g. Tor .onion and Bitcoin addresses are secure and decentralized, but not human-meaningful, because the name is just a hashed representation of a public key.
- Compromise security/ integrity: petname systems (e.g. locally defining names in `/etc/hosts`) are human-meaningful and decentralized, but not secure, as locally defined names are not globally unique.

2.1 Squaring Zooko's triangle using Bitcoin
In January of 2011 Aaron Swartz published an idea called "Squaring The Triangle" [5] in which he disproved Zooko's theory by designing a naming system that fulfills all three properties:

A naming system based on Bitcoin which uses Bitcoin's distributed blockchain as a proof-of-work to establish consensus of domain name ownership.

2.1.1 Bitcoin blockchain
The blockchain is the main invention of Bitcoin [6]. It is a transaction database that contains every transaction ever executed. Every client connected to the Bitcoin P2P network maintains a full copy of the blockchain and thus can find out how many Bitcoins belong to an address at any point in history by traversing the chain of transactions.

A transaction is a signed message that transfers certain amounts of Bitcoins from one or more previous transactions to one or more Bitcoin addresses. Each Bitcoin address is a

doi: 10.2313/NET-2014-08-1_14

representation of the public key of a private-public keypair. The private key of such a keypair is used to sign transaction messages that transfer Bitcoins from the corresponding Bitcoin address. The signed transaction is then broadcasted to every node of the Bitcoin network. Everyone can then verify the authenticity of the transaction using the public key from the sender's address.

These transactions are collected into blocks. A new block includes several recent transactions that have not yet been merged into the blockchain (so-called "unconfirmed transactions"). Once a block is created it is broadcasted and appended to the blockchain and thus becomes part of the Bitcoin history, which means that it will never be changed or removed again (so the transactions of this block are "confirmed transactions" now). Every block in the blockchain contains a reference to its previous block, thus creating a chain from the first block (genesis block) to the current one. The block-reference is a cryptographic hash of the previous block. This ensures the integrity of the chain, as any modification to a block would result in a different hash for the block and thus the reference in the next block would change, resulting in a different hash for every block after.

2.1.2 *Proof of work*

The creation of a block and appending it to the blockchain is called mining. This is a purposely expensive process that requires solving a unique and difficult math problem so that the number of blocks mined each day remains steady. The math problem to solve is used as a proof-of-work, as it is easy to check whether a solution is valid, but it is difficult to find a solution, as this requires a lot of trial and error. In Bitcoin the proof-of-work scheme is SHA-256, which means that the SHA-256 hash of a block's header must be lower than or equal to a specific target value in order for the block to be valid.

2.2 From Bitcoin to Namecoin

Namecoin is based on the code of Bitcoin, it uses the same proof-of-work algorithm and is limited to 21 million coins, but it has its own blockchain beginning with a different genesis block and thus it is a separate currency. In comparison to Bitcoin it has implemented additional RPC (remote procedure call) commands that allow its users to record and transfer arbitrary names (keys) and attach data (values) to those keys in the blockchain by sending special transactions. Those keys are secure and decentralized (as they are stored in the blockchain, so every node can check the validity of the operations on a key) and globally unique and human-meaningful (as they can be arbitrarily chosen), so they are fulfilling all three properties of Zooko's triangle and thus are allowing Namecoin to act as a decentralized naming system.

3. NAMECOIN

The Namecoin blockchain was started on April 18, 2011 and since then on average every 10 minutes a new block is being added. Initially the miners are rewarded with 50 Namecoins for each block, with the reward being halved every 210,000 blocks (approx. every 4 years).

In order to participate in the Namecoin currency a node needs to run a Namecoin client that has a full copy of the Namecoin blockchain and keep it in sync with the P2P network by fetching and validating new blocks from connected peers. The official reference implementation of such a Namecoin client is `namecoind` [10], which can be run in the background as daemon. It automatically connects to the Namecoin network and downloads the blockchain. It also holds the user's wallet, which contains the private keys of the keypairs of the user's Namecoin addresses. The `namecoind` daemon can be controlled by HTTP JSON-RPC commands or via the command-line, e.g.:

```
$ namecoind -daemon
namecoin server starting
$ namecoind getbalance
1.00000000
```

There are several predefined and proposed namespaces for specific use cases as listed in Table 1. For example, by registering a name in the "`id/`" namespace users could use the Namecoin naming system to create online identities and with the help of NameID [14] turn this Namecoin identity into an OpenID, which can then be used to sign into millions of OpenID-enabled websites. Namecoin's biggest and most popular namespace is however the Domain namespace "`d/`" which can be used to register and manage domain names for the virtual top level domain (TLD) "`.bit`".

3.1 Domain namespace

The following sections will describe how the Namecoin system can be used to register a domain in the Namecoin Domain namespace, and how those domains can be accessed with browsers.

3.1.1 *Registering a domain*

A `.bit` domain can be registered using the Namecoin RPC commands `name_new` and `name_firstupdate`, e.g. in order to register the domain `example.bit` the name `d/example` has to be pre-ordered first using `name_new`:

```
$ namecoind name_new d/example
[
  "7004db3cfda8c09945e00b5a793...",
  "abf1c2b6a64c1575"
]
```

This will reserve the domain name by sending a transaction with a hashed version of the domain name, salted with a random value (in this example the random salt is "`abf1c2`..." for transaction ID "`7004db`...").

```
$ namecoind gettransaction 7004db3cfda8c09945...
{
  "amount" : -0.01000000,
  "fee" : 0.00000000,
  "confirmations" : 0,
  "txid" : "7004db3cfda8c09945e00b5a793...",
  "time" : 1400012345,
  "details" : [
    {
```


doi: 10.2313/NET-2014-08-1_14

Namespace	Application	Status
d/<domain>	Domain names for `.bit` TLD	active
id/<identity>	Public online identity system (e.g. addresses for BTC, NMC, email, ...)	active
p/<personal>	Personal namespace for PGP, SSL, identities, etc.	draft
m/<message>	Messaging system for Namecoin users	draft
a/<alias>	Alias system to map a name to another address	draft
tor/<domain>	Domain names for `.tor` TLD for onion websites	draft

Table 1: Namecoin namespaces [9]

```
      "account" : "",
      "address" : "name_new: 13d047d3394...",
      "category" : "send",
      "amount" : -0.01000000,
      "fee" : 0.00000000
    }
  ]
}
```

The additional pre-order step is implemented in order to prevent others from stealing the domain by quickly registering the domain for themselves while the transaction for the domain registration is still unconfirmed, i.e. waiting to be included in one of the next blocks. This is why `name_firstupdate` will only be accepted after a mandatory wait period of 12 additional blocks on the blockchain after the corresponding `name_new`.

Depending on the network activity waiting for 12 blocks generally takes some time between 2 hours and 2 days. Afterwards the domain registration can be finalized using the random value and the transaction ID from the output of the previous `name_new` command and initialized with data. Arbitrary data can be stored for Namecoin keys, but in order to be able to resolve a `.bit` domain the data has to be JSON-encoded according to the schema defined in the Namecoin Domain Name Specification [8], e.g. to resolve a domain to an IP address:

```
$ namecoind name_firstupdate d/example \
> abf1c2b6a64c1575 7004db3cfda8c09945e00b5a793... \
> '{"ip":"127.0.0.1"}'
8b21511aa033ff4f5e219f548df...

$ namecoind gettransaction 8b21511aa033ff4f5e...
{
  "amount" : -0.01000000,
  "fee" : 0.00500000,
  "confirmations" : 0,
  "txid" : "8b21511aa033ff4f5e219f548df...",
  "time" : 1400023456,
  "details" : [
    {
      "account" : "",
      "address" : "name_firstupdate: d/example",
      "category" : "send",
      "amount" : 0.00000000,
      "fee" : -0.00500000
    }
  ]
}
```

In case of a name collision of the `name_firstupdate` command the one with the older `name_new` transaction wins. After the `name_firstupdate` transaction has been added to the blockchain the domain name is registered and valid:

```
$ namecoind name_list
[
  {
    "name" : "d/example",
    "value" : "{\"ip\":\"127.0.0.1\"}",
    "address" : "N1omps5uMutW9xx3gxRmwBaa...",
    "expires_in" : 36000
  }
]
```

Names and values are attached to special coins with a value of 0.01 NMC (Namecoins), stored in the user's wallet (i.e. the user owns the domain). A domain will expire 36,000 blocks (approx. 250 days) after its registration or last update. Updates are performed by creating a transaction with the name's previous coin as input. The Namecoin core code prevents those coins from being used for normal payments [7]. The domain can be updated using the `name_update` command to change its value or reset its expiration period:

```
$ namecoind name_update d/example
'{"ip":"127.0.0.1"}'
```

3.1.2 Resolving a domain

The top level domain `.bit` which is used for the domain names stored in the Namecoin blockchain is a virtual TLD that is not sanctioned by the ICANN (Internet Corporation for Assigned Names and Numbers) and thus is not assigned in the DNS root zone, so regular DNS servers are unable to resolve queries for `.bit` domains and will return a `NXDOMAIN` error instead.

There are various ways how users can reconfigure their systems and/or install additional software in order to be able to lookup `.bit` domains. A comparison of different Namecoin domain lookup software is shown in Table 2.

NMControl. NMControl is a daemon written in python that (amongst other features) acts as a local DNS server. The aim of this software is to allow developers to easily build services on top of Namecoin. When using its DNS server to resolve `.bit` domains it doesn't require trusting any third-party, all data is verified against the local Namecoin blockchain data. Therefore it requires a `namecoind` to be running in the background that has a full copy of the

doi: 10.2313/NET-2014-08-1_14

	local copy of blockchain	access .bit websites (HTTP)	DNS lookup	TLS verify (HTTPS)	supported Operating Systems and Software
FreeSpeechMe	✓	✓		✓	Firefox on Windows / Linux
NMControl	✓	✓	✓		Windows / Linux
MeowBit	✓	✓	✓		Windows
outside DNS suffix		✓	✓		any
outside DNS resolver		✓	✓		any
outside proxy		✓			any

Table 2: Comparison of some Namecoin domain lookup solutions

blockchain in sync with the Namecoin network. NMControl works on Linux and on Windows and is compatible with all Internet applications, not just a web browser. The user has to change the DNS settings of his operating system manually to use NMControl's local DNS server when it is running in order to be able to resolve `.bit` domains.

MeowBit. MeowBit is a Windows application that is based on NMControl. It adds a GUI that manages the included NMControl daemon. The primary difference is that it is easier to use for the end user, as it automatically hooks and unhooks the local name server to the DNS settings of the operating system. Another advantage for the end user is that it is available as a single installation bundle ("`setup.exe`"), so the Windows user doesn't have to take care of installing Python, fetching the NMControl source code, configuring its DNS plugin, etc. It only requires to have the Namecoin wallet software running in the background, which can simply be downloaded as a pre-compiled Windows binary from the official Namecoin website.

FreeSpeechMe. FreeSpeechMe is a browser extension that only works with the Mozilla Firefox browser for Linux and Windows operating systems. It can resolve `.bit` domains to IP addresses from the IP address mappings stored in the Namecoin blockchain. It retrieves the blockchain data via NMControl, therefore it requires NMControl and a Namecoin wallet software (or `namecoind`) to be installed and running in the background. Unlike plain NMControl the FreeSpeechMe browser extension doesn't use NMControl's DNS server to resolve `.bit` domains, so the user doesn't have to touch the DNS settings of his operating system to be able to browse `.bit` domains. Otherwise it implements the same security properties as NMControl, i.e. it does not require trusting any third-party. Additionally it verifies `.bit` TLS certificates against fingerprints stored in the Namecoin blockchain, which allows safe usage of self-signed certificates for browsing `.bit` websites via HTTPS without trusting any third party. This makes FreeSpeechMe one of the most secure ways to browse the `.bit` namespace [11].

Lookup for outsiders. To be able to access `.bit` websites when using systems that currently are unable to run the Namecoin software locally (e.g. mobile devices) some fallback solutions are possible. However using these workarounds permanently or for anything sensitive is strongly discouraged as it introduces a middle man that could possibly censor, hijack or surveil the internet traffic and has to be trusted completely.

One possible solution would be to point the domain search suffix to a publicly available Namecoin DNS suffix gateway. For example if the Namecoin DNS suffix gateway is available through the domain "`namecoin-suffix.dot-bit.org`" it could provide DNS resolution for `.bit` domains with its domain name as suffix: `example.bit.namecoin-suffix.dot-bit.org` would be resolved by the "`namecoin-suffix.dot-bit.org`" server to the IP address of `example.bit` that is stored in the Namecoin blockchain.

The user would then simply add "`namecoin-suffix.dot-bit.org`" to the DNS search domains in his network settings. If he tries to visit `http://example.bit/` his system will query the configured DNS server for `example.bit`, but the DNS server will return `NXDOMAIN`, as the `.bit` TLD doesn't exist in the root zone. Then his system will append the search domain and query the server again for `example.bit.namecoin-suffix.dot-bit.org` which in turn will query the DNS server of `namecoin-suffix.dot-bit.org` who is able to resolve the domain (as explained above). The downside of this approach is that it is insecure: the operator of the Namecoin DNS suffix gateway receives all NXDOMAIN queries, so he is able to log and inject false answers or hijack NXDOMAINs.

Another possibility would be to use a (public) DNS server that resolves `.bit` domains as resolver. There are some volunteer-run DNS servers that can be used for testing purposes, e.g. `dns.dot-bit.org` With this solution the operator of the DNS server will receive all DNS queries, which means that the operator can monitor all queries and fake answers to redirect or hijack any domain, so it is even worse than the DNS suffix solution regarding security.

Finally it is also possible to use a full proxy service that allows HTTP(S) access to `.bit` websites. This does not require any additional software or network setting changes on the client. Regarding security this is the worst solution, as the operator of the proxy server not only can monitor, fake and hijack domains, he also can receive and modify all traffic of the `.bit` website. There are some publicly accessible `.bit` web-proxies, e.g. [12, 13].

3.1.3 Comparison to regular DNS and other alternative name systems

In contrast to the decentralized Namecoin naming system the regular DNS system is hierarchical and centralized, with the Internet Assigned Numbers Authority (IANA) as overall authority for the IP addresses, the domain names, and many other parameters, used in the internet [15]. The ICANN acts as IANA and is responsible for management of the DNS root

zone ("."), the top-level zone of all domain names. It assigns the operators of the top level domain and ensures the maintenance and the administrative details of the individual TLDs. Verisign serves as the root zone maintainer under a cooperative agreement entered with the United States government [15, 17].

Namecoin doesn't have or need such a hierarchy of authorities, all domain records are publicly known to everyone as they are stored in the publicly shared and distributed Namecoin blockchain.

Regular DNS and Namecoin also have fundamentally different business models, DNS registrars have to make a profit from registrations whereas the OpenSource Namecoin project is community based and not profit oriented. This is reflected in a substantial difference in pricing:

Prices for a regular DNS domain name registration from an ICANN accredited registrar (e.g. for the Verisign ".com" TLD) are around $ 10.00 per year. The costs for registering domains in Namecoin vary depending on the NMC/USD exchange rate and on the transaction fees for the Namecoin network:

For every name operation (`name_new`, `name_firstupdate`, `name_update`) the Namecoin transaction fees have to be paid to the miners, otherwise the transaction is unlikely to be included into the blockchain. Currently the standard transaction fees for Namecoin are 0.005 NMC/transaction. The command `name_new` to pre-order a domain has an additional fixed cost of 0.01 NMC. The command `name_firstupdate` initially (at the genesis block) had a network fee of 50 NMC, slowly decreasing over time. This was implemented in order to prevent domain squatting in the early days of Namecoin. Since December 2012 the network fee has fully decreased, so `name_firstupdate` is free today (except for the transaction fees). So the costs to register a new `.bit` domain for one year are 0.015 NMC (`name_new`) + 0.005 NMC (`name_firstupdate`) + 0.005 NMC (`name_update` to prevent it from expiring after about 250 days) = 0.02 NMC. At the current exchange rate of $ 1.79 per NMC (see Table 3) this results in just a few cents per year (approx. $ 0.036). Of course this is just a rough estimate based on the rates at the time of writing - the exchange rates are always fluctuating and might rise or fall by several orders of magnitude when Namecoins are traded on the markets.

Tor hidden services. Tor is an open-source anonymous communication service that implements a practical design for "hidden services", which allows its users to offer services like a webserver without revealing their IP address. In order to connect to such a Tor hidden service an alternative naming system with the pseudo-top-level domain `.onion` is used: Addresses in the `.onion` pseudo-TLD are not human-meaningful, they are an alpha-semi-numeric, hashed representation of the public key used by the hidden service, e.g.: `http://3g2upl4pq6kufc4m.onion/`. Such addresses are not actual DNS names, and the `.onion` TLD is not included in the DNS root zone, only with the Tor proxy software installed Internet programs like browsers can access sites with `.onion` addresses by sending the request through the network of Tor servers.

3.2 Problems

One of the problems of Namecoin is the so-called "domain squatting": Because the cost of registering domains is so cheap those who own Namecoins can register thousands of `.bit` domains anonymously and hold on to forever, as there is no authority instance that could handle disputes and enforce a domain transfer to take it away from them. Many people are using this opportunity to buy up trademarked or copyrighted names [16].

Currently mobile support is also an issue with Namecoin domain name system - there is no support for mobile devices like Android- or iOS-smartphones, as those would somehow have to run a full Namecoin node in the background and keep a local copy of the whole, ever growing blockchain in sync with the Namecoin network, just to be able to lookup `.bit` domains. This requires a substantial amount of resources like memory, storage space and (mobile) network traffic that is not suitable for the hardware of current mobile devices. Additionally the locked-down APIs of the mobile operating systems make it difficult to make Namecoin domain lookups usable for all applications, e.g. an Android phone would have to be rooted to be able to change the system's DNS resolver address to a different, `.bit`-capable (local) DNS server.

Another possible source of problems is the code quality of the Namecoin core, e.g. in October 2013 a severe bug was found in the name verification code that allowed everyone to take an already registered name and update it with a new value, even though this name did not belong to them. There was no enforced integrity of the key value pairs in Namecoin before version Q.3.72, which basically defeated the entire purpose of Namecoin. This was quickly fixed and a new Namecoin version was released the next day, resulting in a hardfork of the Namecoin blockchain after block 150,000 [18]. This means that there was an out of bound agreement to change the Namecoin name verification rules, so that transactions overwriting the names of others won't be accepted any more after this block.

Namecoin shares all structural theoretical weaknesses with Bitcoin, e.g. if an Attacker has a lot of computing power and controls more than 50% of the whole Namecoin network's mining power it allows him to exclude and modify the ordering of transactions. Thus he will be able to block transactions from being confirmed and prevent other miners from mining any valid blocks while he is in control. The attacker can also change the (recent) blockchain history: he can modify an existing block and start mining a blockchain fork that builds on top of the modified transaction. Since the attacker has more computing power than the rest of the network combined he can generate blocks faster than the rest of the network. Eventually his private fork will become longer than the real blockchain branch. When this happens his fork will become the new "official" blockchain per definition, as it is the longest branch now. The rest of the network will switch to his branch and continue mining there. This attack could be used for double-spending coins or (Namecoin specific) to steal a domain registration:

1. Modify the block that contains the `name_firstupdate` transaction of the domain to steal:

doi: 10.2313/NET-2014-08-1_14

(a) Remove the `name_firstupdate` transaction.

(b) Add own `name_new` transaction that pre-registers the domain for the attacker.

⇒ This modification creates a private fork of the blockchain.

2. Mine at least 12 new blocks on top of the private fork without including the previously removed `name_firstupdate` transaction again.

3. Add own `name_firstupdate` transaction with the matching random value of the pre-registration from step 1.(b) into the next block.

4. Continue mining blocks for the private fork until it becomes the longest branch in the network.

5. Now the domain is registered to the attacker.

6. The real, previously removed `name_firstupdate` transaction is now invalid, as the attacker's registration took its place.

3.3 Statistics

Following are some facts and statistics about Namecoin:

- According to Table 3 Namecoin is currently the 6. biggest mineable cryptocoin.
- The exchange rate for NMC/USD fluctuated by a factor of 8 during a period of less than 6 months
- Up until Aug 3, 2014 more than 9.4 million Namecoins have been created [20].
- The Namecoin blockchain contains more than 190,000 blocks.
- The full blockchain and its index files require more than 1,900 MB to be stored.
- Currently there are 122,772 non-expired names registered in the "`d/`" namespace (TLDs `.com`: 113,639,892 / `.de`: 15.743.799)
- 108,114 (88%) of those are valid `.bit` domain names.
- 6,790 (5.5%) of those can be resolved to a website [20].
- 429 (0.3%) of those are unique (mapped to unique IP addresses) [20].

4. CONCLUSION

This paper has outlined how the Bitcoin-based Namecoin system can be used as an alternative to the hierarchical and centralized DNS and how this could potentially prevent and circumvent censorship. However the practical use cases are currently limited by several problems, which makes this system unlikely to be adopted by a signifcant number of internet users at this time. Due to this nicheness even more problems arise, like the large amount of name squatting, as only 0.3% of all currently registered domain names can be resolved to unique websites.

#	Name	Market Cap	Price per coin
1	Bitcoin	$ 7,305,063,919	$ 566.380000
2	Litecoin	$ 286,957,784	$ 9.800000
3	Darkcoin	$ 44,446,712	$ 10.140000
4	Peercoin	$ 36,504,715	$ 1.700000
5	Dogecoin	$ 31,191,323	$ 0.000378
6	**Namecoin**	**$ 16,161,798**	**$ 1.790000**
7	BitShares-PTS	$ 6,951,251	$ 4.230000
8	NeutrinoCoin	$ 6,914,311	$ 0.032882
9	Quark	$ 4,056,502	$ 0.016361
10	Vertcoin	$ 3,767,091	$ 0.719721

Table 3: Top10 Crypto-Currency Market Capitalizations [19] (Jun 15, 2014 7:15 AM UTC)

5. REFERENCES

[1] *Turkey's YouTube and Twitter bans show a government in serious trouble*. Alev Scott, The Guardian, March 2014. `http://www.theguardian.com/commentisfree/2014/mar/28/turkey-youtube-twitter-ban-government-trouble`

[2] *DNS Cache Poisoning in the People's Republic of China*. ViewDNS.info, September 2011. `http://viewdns.info/research/dns-cache-poisoning-in-the-peoples-republic-of-china/`

[3] *Names: Distributed, Secure, Human-Readable: Choose Two*. Zooko Wilcox-O'Hearn, 2001. `https://web.archive.org/web/20011020191610/http://zooko.com/distnames.html`

[4] *Zooko's triangle*. Wikipedia, 15.06.2014. `http://en.wikipedia.org/wiki/Zooko's_triangle`

[5] A. Swartz. *Squaring the Triangle: Secure, Decentralized, Human-Readable Names*, Jan 2011. `http://www.aaronsw.com/weblog/squarezooko`

[6] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. `https://bitcoin.org/bitcoin.pdf`

[7] *Namecoin FAQ*. `https://dot-bit.org/FAQ`

[8] *Namecoin Domain Name Specification*, version 2.0. `https://wiki.namecoin.info/?title=Domain_Name_Specifica`

[9] *Namecoin Namespaces*. `https://github.com/namecoin/wiki/blob/master/Namespace.m`

[10] *namecoind*, sourcecode of the Namecoin-client reference implementation. `https://github.com/namecoin/namecoin`

[11] *FreeSpeechMe*. Software plug-in for Firefox that allows people to effortlessly view `.bit` websites. `https://directory.fsf.org/wiki/FreeSpeechMe`

[12] *dotbit.me proxy*. `https://dotbit.me/proxy/`

[13] *bit.no.com*. namecoin web proxy. `http://bit.no.com/`.

[14] *NameID*. Crypto-OpenID. `https://nameid.org/`.

[15] J. Postel. Rfc 1591, Domain Name System Structure and Delegation, 1994.

[16] J. Prasanna, S. Prakash, Nikhil, S. Selvan. *.bit squatting*, Cyber Security & Privacy Foundation, Jan 2014. `http://cybersecurityprivacyfoundation.org/Namecoin_bit.pdf`

[17] *Root Zone*, ICANN Wiki, 15.06.2014. `http://icannwiki.com/index.php/Root_Zone`

[18] *Namecoin was stillborn, I had to switch off life-support*, Michael Grønager, Payward Inc., 15.10.2013.

https://bitcointalk.org/index.php?topic=310954.0
[19] *Crypto-Currency Market Capitalizations.*
http://coinmarketcap.com/
[20] dotbit.me: *The simple way to a .bit address.*
https://dotbit.me/
[21] BitcoinWisdom BTC-e NMC/USD.
https://bitcoinwisdom.com/markets/btce/nmcusd

doi: 10.2313/NET-2014-08-1_14