Namecoin as alternative to the Domain Name System

Xander Lammertink
Author, UvA System and Network Engineering
xander.lammertink@os3.nl

Marco Davids
Supervisor, SIDN Labs

Abstract: This paper researches if Namecoin could be used as an alternative to the DNS. Namecoin offers the same functionality as Bitcoin, but is also able to store data. It is used to store domains, identities, product meta data, etc. We have seen that the DNS is suffering from weaknesses and Namecoin is able to address these under certain conditions. Organisational roles will be affected by switching from the DNS to Namecoin: some will change, some will disappear but new roles will arise as well. The switch has been discussed as well, we found two transition scenarios that are possible.

1. Introduction

The Domain Name System (DNS) has been specified in 1983 and has been the de facto naming system on the Internet ever since. It has proven its robustness and sustainability, but some weaknesses have been discovered over time.

Numerous additions have been implemented to keep the DNS running. Anycast is used to distribute the load of the 13 static root-server addresses over multiple servers spread all over the world, DNSSEC has been specified to ensure the authenticity of the response data, DNS Curve provides authorisation and encryption of DNS responses and many more additions can be added to this list.

Instead of continuing to fix all the “problems” that have been encountered over time, some thought it might be better to start from scratch or from a whole different perspective to address all these challenges.

An example of a system that tries to do this is Namecoin, a distributed open-source information registration and transfer system based on the Bitcoin cryptocurrency.

1.1. Research Questions

This research is all about the potential of Namecoin being an alternative to the Domain Name System.

We would like to know the differences between the DNS and Namecoin, if it can match the robustness of the DNS and what the consequences are for the roles in the DNS.

The main research question is: *What is the potential of Namecoin as an alternative for the Domain Name System?*

This question has been divided in multiple subquestions that together answer the main research question. The sub-questions are:

- *How does Namecoin work?*
- *What are the current shortcomings of the DNS system?*
- *Which of the shortcomings of the DNS does Namecoin address?*
- *Can Namecoin match the robustness of the DNS?*
- *What are the consequences for the different organisational roles like DNS operators, registrars, (root) registries, etc.?*
- *How would a transition scenario from the DNS to Namecoin look like?*

1.2. Related Work

Up to now there is not much related work on this topic. Some research has been done on using Namecoin for certain purposes and an informational RFC (Request for Comment) has been written about the weaknesses of the DNS.

F. Jacobs [1] did research about Namecoin and MinimaLT to provide better confidentiality and authentication on the Internet. Instead of improving the currently used protocols like DNSSEC, TACK and DANE, they proposed to use MinimaLT with Namecoin.

T. Melin and T. Vidhall [2] researched if Namecoin could be used as an authentication mechanism for public-key cryptography. They investigated the flaws and consequences in current public-key cryptography and presented Namecoin as alternative to replace the currently used certificate authority system.

In RFC 3833 [3] some of the well-known weaknesses of the DNS have been discussed. At the time this RFC was published, DNSSEC was being developed although no real design goals were set. By discussing the weaknesses of the traditional DNS it was possible to see what DNSSEC improved on the current situation. Although Namecoin was not discussed in this RFC, it can be useful to see what weaknesses of the DNS can be addressed by using Namecoin.

2. Bitcoin

Namecoin is a fork of Bitcoin, the distributed digital cryptocurrency, with minor changes (± 400 lines of code) and extra functionality [4]. To understand Namecoin it is important that the Bitcoin concept is familiar. Therefore a start will be made by describing the Bitcoin concept. In section 3 the differences between Namecoin and Bitcoin will be discussed.

This explanation is not intended to cover all the ins and outs of Bitcoin, but that's also not necessary for the understanding of Namecoin. The interested reader is advised to read [5] to get a more detailed explanation of Bitcoin.

In Bitcoin there are four topics that form the core of the cryptocurrency: transactions, wallets, mining and the blockchain. Transactions are used to transfer Bitcoins (the currency in Bitcoin, also denoted as BTC) from one to another. A wallet is no more than a set of keys used to sign certain transactions. All transactions are stored in blocks, created by miners that compete with each other to submit their blocks first to retrieve Bitcoins. Every block links to the previous block using hashes and contain transactions that link to transactions from other blocks.

As one might have noticed already, there is no database that stores how much money is in a wallet. Instead, by looking at all historical transactions that are related to a wallet, a total amount of Bitcoins can be calculated. This can be done by others as well, because all transactions in Bitcoin are available to everyone.

2.1. Transactions

Transactions are used to transfer Bitcoins from one to another. This is done by using addresses that are usually based on public keys. The owner approves a transaction by signing it with its private key. By using the public key of the owner, everyone is able to check the signature and thereby confirm a transaction. Most addresses are RIPEMD-160 encoded SHA-256 hashes of the public key. Some transactions contain unlocking or locking scripts to set conditions on processing the transaction or spending it (e.g. stating the transaction can only take place after a certain date or when M out of N keys have signed the transaction).

A transaction exists out of (multiple) inputs and (multiple) outputs. The inputs are unspent transactions outputs (UTXO) gathered from previous incoming payments. Like in physical money, one takes one or more UTXOs totalling the amount to spend (or more) as input. The outputs are the amount of Bitcoins to spend to the address of the receiver, possibly more amounts to other receivers and the change minus a transaction fee to the originating address. The sum of all transaction inputs minus the sum of all transaction outputs is the transaction fee that is taken by the miners that include the transaction into the blocks they produce. The current transaction fee is 0.0001 Bitcoin per kilobyte. To prioritize a transaction it is possible to increase the fee.

2.2. Wallets

Wallets contain one or more cryptographic keys. Using these keys transactions can be made or unlocked. There are deterministic, undeterministic and hierarchical deterministic wallets. The first type contains private keys that are derived from a single key using a one-way hash function. Undeterministic wallets have a collection of randomly generated private keys. The hierarchical deterministic wallets have parent keys that are used to derive multiple child keys. From the child keys it is possible to generate grandchild keys. This is done using a one-way function, making it impossible to derive the parent key from the child keys.

When transactions are made, the transactions will be submitted to the connected neighbours (can be any node within the Bitcoin network) and the neighbours send it to their neighbours, spreading it through the peer-to-peer network. Every node receiving a transaction will check the signature of the transaction before sending it to his neighbours. Invalid transaction will not be spread any further. Miners will receive the transaction as well and put it in a queue so they can process it.

2.3. Mining

The goal of mining is to secure the bitcoin system against fraudulent transactions or transactions that spend the same Bitcoins multiple times. Approximately every 10 minutes a block is mined by a miner. The miner receives an award (starting with 50 BTC per block, decreasing by 50% every 210.000 blocks) and the transaction fees of all transactions for every block they mine. This is done by adding a transaction to themselves. The mined blocks are distributed through the network in the same way as transactions are distributed.

Creating blocks is a compute intensive task. Every block is made by adding transactions from the queue to a new block, including a transaction that contains the mining award and transaction fees. The next step is to calculate a hash over the header repeatedly, changing one parameter (the nonce) every time. This process is repeated until the hash is matching the criterion that is set. When the hash matches the criterion, the block is mined and can be distributed throughout the network.

There is one criterion that the hash should match: be below a certain value. This value is determined by the difficulty. When the difficulty is increased, the hash should match a lower value. Increasing the difficulty will lower the chance that a hash matches the criterion, requiring more time and/or processing power. This is called the “proof-of-work” system. A miner that can provide a block with a nonce that matches the difficulty can prove it has done a lot of work to calculate that block. Because the total processing power in the Bitcoin network differs, the difficulty is re-adjusted every 2.016 blocks to make sure every 10 minutes a block will be mined.

2.4. Blockchain

When a block has been mined and is sent to the network, nodes will try to verify if the nonce results in a matching hash. If the hash matches and the transactions are valid as well, the block is considered to be valid and will be added to the blockchain.

Because the transactions in a block are linking to transactions in previous blocks and the new block contains the hash of the previous one, we can say that the blocks are chaining together, forming the blockchain. The blockchain can be used to retrieve the amount of money linked to an address, create new payments, and can be used for many more purposes.

3. Namecoin

Namecoin is a fork of Bitcoin, meaning that all functionality within Bitcoin can also be found in Namecoin. Only a few changes have been made to the Bitcoin code base and extra features have been added to it [4]. The most important change is that Namecoin is able to store data other than just transactions in the blockchain.

In this section we will start with the motivation of developing Namecoin followed by how it provides all the properties that are desired in a naming protocol. Then we discuss the features that are in Namecoin, the process for registering domain names, which top-level domain (TLD) is used and the delegation of (sub-)domains.

3.1. Motivation

The motivation to start Namecoin is primarily to have an alternative to the traditional domain name system. Namecoin does not rely on centralized authorities making it censorship-resistant. They also claim to provide security (by replacing certificate authorities), privacy and and less latency.

3.1.1. Censorship-resistance

Currently the DNS is decentralized. This offers organization with much power the possibility to control the content of the system. An example provided by Namecoin is the SOPA, a law in de United States to prevent piracy. The SOPA mandated to send NXDOMAIN responses to queries that request certain domain names. By many people this was seen as censorship.

Regardless of the discussion if this is censorship or not, applying these actions can be used to create censorship. A distributed system like Namecoin will make it hard, if not impossible, for authorities to block domain names this way. Making changes is only possible by the owner of the private key which is used to register a domain. This is what Namecoin calls “censorship-resistant”.

3.1.2. Security

The DNS is used to provide human-meaningful names instead of direct IP addresses to access a system. By making the DNS secure, the system that is accessed is not secured. The only guarantee that can be given is that a certain IP address belongs to a certain domain name.

Securing websites is done by applying an SSL connection to encrypt the HTTP traffic. The SSL connections used in HTTPS builds on certificates that need to be trusted by the client to prove that the data has not been altered.

To let the client accept certificates, a user can manually accept a certificate or a trusted certificate authority (CA) signs the certificate of the server. When the user/application trusts a certificate authority, the certificates signed by that CA are trusted as well.

The problem with CAs it that the whole system relies on trustworthy CAs. If a CA gets compromised or makes a mistake, someone else is able to impersonate many websites. For this reason a lot of effort is made in securing CAs before they get accepted by browsers and operating systems. This is why many certificate authorities ask money for their services.

Namecoin is able to store the fingerprint of a certificate and therefore one could use Namecoin instead of a CA to trust the certificate of a website. This way a user can validate the certificate using the fingerprint that is stored in the blockchain, which is trusted because of its proof of work.

3.1.3. Privacy

As we will discuss in section 4.1.1, it is possible for an attacker to see DNS packets and their content using a man-in-the-middle attack. By reading the content it is possible to deduct the behaviour of a user, like what sites are accessed or what services are used. Even if DNSCurve is used, which encrypts the content of the packets, it is possible to make an educated guess based on the destination IP address of a query.

Namecoin can solve this problem, assuming that the blockchain is available at the client. The client can simply perform the lookup locally by searching for the domain in the blockchain. There is no need to send queries over the Internet.

If the blockchain is not available at the client, the client still needs to send queries to a remote server to do the lookup. In that case queries are sent over the Internet in DNS packets, which makes it possible to see inside the packets again. Using DNSCurve between the client and Namecoin server could be a solution because it encrypts DNS messages, making the two factors of guessing disappear (see section 4.2.2).

3.1.4. Faster

A DNS query that cannot be answered from local cache needs to be resolved by asking remote name servers. A start is made by asking root servers for the name server of the TLD, the TLD will be asked for the name server of the sub-domain, etc. When Namecoin is used, all domain names are locally available. There is no need to ask (multiple) servers over the network. This could result in faster lookups.

Unfortunately the performance of Namecoin and DNS have not been compared with each other. Namecoin claims that the DNS resolves domain names in an average of 100 ms and Namecoin in just 3 ms. Looking at research on DNS resolvers [6], we can see that the claim of 100 ms looks realistic. However, similar research on the performance of Namecoin is not available, making it is impossible to compare the claim with Namecoin's performance. Based on common sense it seems very likely that Namecoin lookups are significantly faster then lookups in the DNS because queries do not have to traverse the Internet multiple times. Because of time constrains and the scope of the project no performance measurements have been done to verify the claim.

Another part in which DNS is pretty slow is updating records. Since caching is actively used to speed up performance it might take a while before everyone is using the same updated data. Where an update in DNS usually takes multiple (up to 8 hours) hours to be processed everywhere, Namecoin can be faster.

A domain name is registered when the *name_firstupdate* transaction is sent. This transaction can be sent after waiting 12 blocks from the *name_new* transaction. Since it takes approximately ten minutes to mine a new block, a domain can be registered in roughly two hours.

Updating an existing domain takes the same amount of time. Twelve blocks after a transaction has been sent it should be spread through the whole Namecoin network. Taking the average mining time of ten minutes per block, this would also result in roughly two hours.

3.2. Zooko's triangle

Wilcox-O'Hearn [7] described the three properties that are desired to have in naming protocols. The three properties are:

- Human-meaningful: A name that can be remembered and/or is chosen by a user.
- Decentralized: No need for a central authority that determines the mapping of a name.
- Secure: A name can only be mapped to a single entity. It should not be possible to map an item to more than one entity.

Wilcox-O'Hearn claimed that a naming protocol can have up to two of these desired properties. To illustrate this Zooko's triangle was created (see Figure 1). No matter what naming system one can think of, according to Wilcox-O'Hearn it will have at most two of the desired properties. An example: Tor is a system that is decentralized and secure, but unfortunately it lacks the capability of using human-meaningful names.

Fortunately Wilcox-O'Hearn was wrong. A few naming systems are now able to include all properties of Zooko's triangle, thereby squaring the triangle. Namecoin is one of these systems because it can provide human-meaningful names, is decentralized and secure.

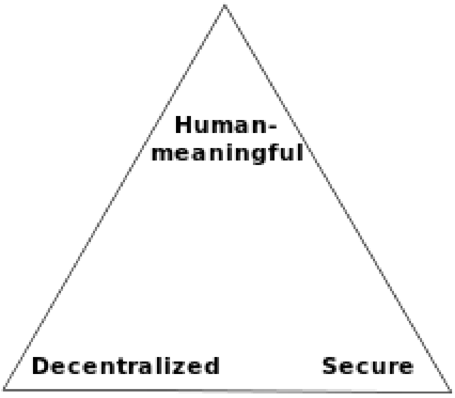

Figure 1: *Zooko's triangle, claim: any naming protocol can have up to two of the desired properties. Namecoin covers them all.*

3.3. Features

Namecoin has been developed in a way that makes it possible to add more features to it. To make a distinction between these features, every feature is identified with a prefix (e.g. "id/"), also known as an application specifier. The two main features are registering domains and registering identities.

The application specifier "d/" is used to register domain names under the ".bit" top-level domain and the "id/" prefix is used to register identities. Some examples of features that are not well-known or still under development [4] are:

- Onename ("u/" or "i/"): Onename is a protocol for a decentralized identity system with a user directory comprised of entries in a decentralized key-value store. [8]
- Physical unclonable function ("puf/"): store signatures for physically unclonable objects (non-expiring values that cannot be changed). Although the values are non-expiring, the values can be revoked.
- Product meta data ("p/"): store meta data of products in the blockchain.
- Proof of existence ("poe/"): store hashes of the actual data, e.g. a SHA256 hash of a document, image, sound or any other digital data.

3.4. Top-Level Domain

In RFC 6761 special-use domains have been specified. The document describes what special-use domain names are, when such names are appropriate and what the procedure is of reserving a special-use domain name. If a domain name has special properties that affect the way hardware and software implementations handle the name, then that domain name is a candidate to be a special-use domain name. [9]

Because Namecoin works completely different from the traditional DNS in the way software is implemented, it is a candidate for a special-use domain name. A draft has been created to register a set of special-use domain names for use with peer-to-peer (P2P) systems [10]. In this draft an attempt has been made to register the following pTLDs (special-use top-level domain names for use with P2P systems): GNU, ZKEY, ONION, EXIT, I2P and BIT. The BIT pTLD was proposed as a name space where names can be registered via transactions in Namecoin. The proposed draft was created in November 2013, but expired in July 2015.

After the draft for the peer-to-peer systems, a more specific draft has been created to register a special-use domain name to use with the Namecoin system [11]. This draft only proposed the BIT pTLD as name space for Namecoin and expired December 2015.

Although the proposals to put BIT in the special-use domain names list are not working out as expected, Namecoin is still using the virtual .bit top-level domain. However, to become a mature naming system, the pTLD must certainly be registered. This way Namecoin will not interfere with the DNS in any way.

3.5. Registering Domain Names

Registering .bit domain names can be done in two steps. First the *name_new* operation needs to be executed. This operation will pre-register the domain which is necessary to prevent others from registering your domain quickly when they see your transaction. The output of this command is the hash value of the domain name and a random hexadecimal number (the salt that is used in the hash). The costs associated with the *name_new* operation are the network fee of 0.01 NMC (Namecoins) and the transaction fee. The network fee will be destroyed.

The second step is sending the *name_firstupdate* transaction. In this step the domain name becomes registered and one can add records to it. The only cost associated with this transaction is the transaction fee for the miners to process the transaction. Before *name_firstupdate* can be executed one has to wait 12 blocks after the *name_new* operation, this ensures no one will see the second transaction before the previous one.

There is also a third step to renew, update or transfer a domain. In this step the *name_update* operation is executed. Domains are valid for 36.000 blocks (corresponding to roughly 200-250 days) after this period anyone is able to register the domain again. Executing the *name_update* operation resets the validity of the domain name.

3.6. Delegation

As in the traditional DNS it is possible to delegate parts of .bit domains to other entities. In the DNS this is done using an NS record pointing to the IP address of the authoritative name server of that part of the domain. In Namecoin this is not possible due to the distributed design of the system.

Instead of an NS record, Namecoin uses the *delegate* record type. The *delegate* record type delegates the authority of one domain to another (sub-)domain. The provided address will have authority over the specified domain.

A special application specifier “s/” has been proposed for delegations. It has been proposed to distinguish non-resolvable domain data from domain names [13]. Although the “s/” application specifier is proposed for delegations, it is also possible to delegate sub-domains to an address starting with the “d/” or “dd/” prefix.

Another way of delegating domains is using the *map* record type. This record type is delegating in the same way as the *delegate* record type, but it only maps a sub-domain to another address instead of delegating the complete domain.

It is also possible to transfer a domain to someone else. One could issue the *name_update* command, ending with the address of new owner. This allows people to sell their domains as well.

3.7. Domain Name Syntax

Domain names in Namecoin have to apply the same syntax requirements as stated in RFC 1035: “The labels must follow the rules for ARPANET host names. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphen. There are also some restrictions on the length. Labels must be 63 characters or less”

[12]. Internationalized domains are encoded using the IDNA standard [13].

3.8. Resource Records

The values of a domain are registered in UTF-8 encoded JSON objects with a maximum size of 520 bytes. All entries are case-sensitive. Many of the resource record (RR) types that are available in the DNS are available in Namecoin, but often with a different name associated to it. A list of all possible entries and their DNS equivalents can be found in appendix A.

4. The Domain Name System

Now we are familiar with the working of Namecoin and know what it is trying to accomplish, we will take a look at the domain name system. We will start by identifying the weaknesses of the DNS using RFC 3833. When the weaknesses are known we will look at Namecoins defence against these weaknesses and how it is improving on it.

4.1. Request for Comment 3833

Request for Comments (RFC) 3833 [3] is an informational RFC document that has been created to determine if DNS Security Extensions (DNSSEC) was meeting its design goals. At the time that the RFC was published there were no specific design goals for DNSSEC. The document tries to clarify if DNSSEC is a useful tool to defend against some well known DNS threats.

RFC 3833 will be used to determine a number of well-known attacks from which the DNS is suffering. In this section we will describe the attacks and find out to what extend Namecoin is defending against these attacks.

4.1.1. Packet Interception

The first threat that will be covered is packet interception attack. Because the DNS is using unencrypted packets to communicate with servers it is very easy for an attacker to intercept the DNS traffic using a man-in-the-middle attack. The attacker listens to the traffic on the path between the client and server. It can decide to let all requests pass through and possibly analyse the behaviour, but it might be more interesting to alter the response data (RDATA). The responses can for example refer to the attacker his IP address instead of the IP address that the authoritative name server would serve.

Because the DNS originally does not provide any end-to-end integrity checking, the client will not notice any difference between an authoritative or altered answer. DNSSEC could provide this integrity, but is still not used everywhere.

4.1.2. ID Guessing and Query Prediction

As discussed in section 4.1.1, the DNS primarily relies on unencrypted UDP packets that are easy to spoof. There are a few things that make spoofing DNS packets a bit more difficult: there is a 16 bit ID field in the DNS header and there are 2 8-bit port fields (client and server side) in the UDP header. This totals to a number of 2^{32} unique possibilities. These possibilities can even be brought down to 2^{16} when the UDP ports are known and even further when the attacker is able to predict the behaviour of the client to a certain extend.

When ID guessing is combined with knowledge about queries (predicting the resolver behaviour) this attack will be hard to detect, making it easier to implement. Although the execution of this attack is more difficult than the packet interception attack, it is more feasible because it is not necessary to be in the middle of the communication.

4.1.3. Name Chaining

In name chaining a victim issues a DNS request and the attacker responds with modified data. The victim might even be asking for another name since the attacker is just using this query to inject false information about some other domain name. The modified responses often include an NS, CNAME or DNAME record to refer the victim to a name server controlled by the attacker.

Once the response is accepted by the DNS resolver, the resolver probably caches the answer for a certain period to increase performance. If the same query is issued before the TTL (time-to-live) expires, the resolver will respond with cached data instead of asking name servers again. This will speed up the lookup process. For an attacker this is very useful because the attack needs to be executed only once to work for a long time.

4.1.4. Betrayal by Trusted Servers

Most network devices are configured with a stub resolver that sends recursive DNS queries to a trusted resolver that executes the resolving process for the client. Choosing the DNS resolver can be done manually, but is often arranged by the user's ISP or network operator using the DHCP protocol. Once the resolver is chosen, the computer trusts that server and expects it to return valid data.

If the client is intentionally or unintentionally configured to use a malicious resolver (for example by attacking the DHCP protocol) or the trusted server is compromised, queries are sent "voluntarily" to an attacker. Although this is not an attack on the DNS protocol, this approach can be used by an attacker to perform a man-in-the-middle attack.

4.1.5. Authenticated Denial of Domain Names

Now we know that DNS responses can be altered to show different results, we can also take this to a higher level. So far we mainly looked into changing the response data to refer clients to other servers.

This is one of the options, but it is also possible to extended this by denying the existence of domain names. Instead of changing the answer to refer to another IP address, one can serve an NXDOMAIN result code which tells the resolver that the domain it was looking for does not exist. This can be executed using many spoofing attacks.

4.1.6. Denial of Service

As any service on the network, the DNS is vulnerable to denial of service (DoS) attacks. DNS servers are at risk of being used for an amplifier attack in which spoofed queries are fired at the server. The spoofed queries usually require little bandwidth to send and result in answers that are significantly larger in size than the query.

Attacking authoritative name servers can result in domain names not being able to resolve (from that point, down in the tree) from all over the world. Attacking resolvers can result in all clients relying on that resolver being unable to resolve any existent domain name.

The impact of this attack can be huge because the internet is extremely depended on domain names. Some DoS attacks that have been executed have seriously affected the internet access of my many users in a negative way (examples: [14], [15] and [16]).

4.1.7. Wildcards

Wildcard RRs can be thought of as instructions for synthesizing resource records [17]. To determine if a wildcard RR can be synthesized, the following requirements must be met: the resource record that is requested does not exist and a matching wildcard must be available.

DNS name servers will determine if a wildcard can be synthesized. If synthesizing is possible, it will return a CNAME record referring the requested domain to the synthesized domain name. In the standard DNS implementation it is not possible to verify if a wildcard is correctly synthesized, nor to see the difference between a CNAME and a synthesized wildcard record.

4.2. Defence of Namecoin

Due to the distributed design of Namecoin, most of the attacks that are listed in RFC 3833 are no longer applicable when the blockchain is locally available. The the authenticity of the data is assured by the blockchain itself that exists out of blocks with proof of work which are dependent on previous blocks. All transactions are verified independently.

In this section we have made a separation between a locally and remotely stored blockchain. Local blockchains are the preferred way, because this offers many benefits, but sometimes it is not feasible to store the complete blockchain at the client. This leaves the only other option: storing the blockchain at a remote server.

4.2.1. Locally Stored Blockchain

Because the blockchain can be stored on every client, there is no need to query remote servers (which would be another Namecoin node) over the network. A client will be configured to send DNS queries to port 53 of the localhost where NMControl (the Namecoin resolver) is listening. Man-in-the-middle attacks that require DNS queries to be sent over a network, do not work any more. This means that the packet interception, ID guessing/query prediction and name chaining attacks are not possible any more, unless the attack can be executed on inter-process communication.

Storing the blockchain on the client also has the benefit of the client becoming a full resolver instead of just having a client stub that queries another resolver. Mechanisms like DHCP, on which many clients rely, are not needed to automatically configure a resolver and the trust in an external resolver is not necessary any more. The chance on a betrayal by trusted servers attack is therefore much smaller since you only have to trust yourself.

DoS attacks are very hard to execute when Namecoin is used. Again, storing the blockchain locally ensures that targeting specific servers with DoS attacks will not result in (a big part of) the network going down. The distributed design ensures that the system has no single point of failure any more.

Another DoS attack in Namecoin could executed by abusing the property that all transactions are distributed to all nodes in the peer-to-peer network. By sending many bogus transactions to multiple clients, one could possibly cause a blockchain melt-down when the transactions are distributed to all nodes. Fortunately this is not possible because all transactions are checked by every node in the Namecoin network. Valid transactions require relatively much processing power to create and invalid transactions will not be sent any further in the network, making a DoS attack very costly.

An additional benefit of storing all existent domain names at the client is that the client is able to determine which domains are existent and which are not. The denial of domain names can therefore be verified. When a query is synthesized by a wildcard, the client has verified the two requirements for synthesizing wildcards.

4.2.2. Remotely Stored Blockchain

For some reasons it might not be feasible to store the blockchain at the client. Especially on mobile devices the size of the blockchain (currently 4 GiB) could be a real deal breaker. A problem that comes with having a remote blockchain is that clients need to query servers over the network to get provided with data.

The solution that is currently offered by Namecoin is to let NMControl listen to port 53 of the outbound interface. This way a client can send DNS queries to the NMControl server like it would do to any regular DNS resolver. Sending queries over the network will have consequences when it comes to the attacks listed in section 4.1 because the standard unencrypted DNS packets are used again.

Since Namecoin allows DS records to be stored using *ds* entries, one could think that DNSSEC could solve some of the integrity problems. Unfortunately this is not the case, because DNSSEC relies on a chain of trust, starting from the root, down to all the delegated subdomains. Due to the fact that the .bit domain is a virtual TLD, there are no (DS) records of the .bit domain in the root zone. This means that the root of the chain of trust is already broken.

Even if there would be a well-known public key for the .bit TLD, the sub-domains of the TLD (the domains that are registered in Namecoin) would need a DS record of their domain in the TLD. Putting the DS record in the .bit TLD would require an authority that is able to execute this, which is completely against the principles of a distributed naming system that should not be controlled by authorities.

A solution must be found to secure the last mile (from the client stub to the DNS resolver). Examples to do this could be using an existing technique like DNSCurve or implementing a new protocol that replaces the DNS queries to lookup information in the blockchain. This would require more research.

Using the by Namecoin proposed way of storing the blockchain remotely will introduce the same weaknesses as in the traditional DNS. Packet interception and ID guessing & query prediction are possible. This allows attackers to implement name chaining, authenticated denial of domain names and wildcard synthesizing. Next to these attacks, the betrayal by trusted servers and denial of service attacks are possible as well.

5. Transition Scenarios

In the previous sections we focussed on the features and possible improvements that Namecoin offers and why one could choose to switch to Namecoin. Something that has not been discussed is how to switch from the DNS to Namecoin. What are the possible transition scenarios? We can split the transition up into two parts. At first the domain names need to be made available in Namecoin and secondly the resolvers need to switch from the DNS to Namecoin.

5.1. Domain Names

Making domain names available in Namecoin is relatively simple. One needs to retrieve Namecoins (e.g. by mining or via exchanges) and register domain names using a client application (e.g. Namecoin-Qt). Registering domain names in Namecoin can be done while the domain names in the DNS are still available. This way the domain names are available through both naming systems. The process of registering domain names has been discussed in section 3.5.

5.2. Resolving

Basically there are two options when it comes to resolvers (or client stubs). One could choose to make a "hard switch" or to resolve domains using both systems in parallel. In the hard switch scenario one will continue to use the DNS up to a certain point, after this point only Namecoin will be used to look up domain names. In the other scenario, where both systems can be used in parallel, the resolvers will be able to resolve queries for both Namecoin and the DNS.

5.2.1. Hard Switch

We will start by discussing the hard switch scenario. In this scenario the DNS will still be used for all queries. During this time, the domain names that are in the DNS will be made available in Namecoin. When all domain names are available in Namecoin a certain point in time will be chosen to update the resolvers (or client stubs). After the switch only Namecoin will be used.

Instead of choosing a fixed date, it might be better to use a larger time frame (e.g. a week or a month) in which both systems can be used. This gives users and system administrators more time to update all clients. During this time frame there will be clients that only use Namecoin and clients that only use the DNS. This requires that updates to domain names need to be made available in both systems.

Theoretically this sounds like a clean transition that is easy to accomplish, but practice shows that it is not as easy as it seems. Various switches in important protocols, think NCP to TCP/IP and IPv4 to IPv6, have been hard to accomplish or are still ongoing. Users will also experience problems when they fail to switch in time, it will leave them with a non-working system or out-of-date information.

5.2.2. Parallel

The second option, in which both the DNS and Namecoin work in parallel is more likely to accomplish. Because Namecoin domain names are ending with the ".bit" extension it is very easy to make a distinction between domain names originating from the DNS or Namecoin. Using this knowledge, client stubs can choose which system to use for lookups.

When the requested domain name ends with the .bit extension, the client stub can look up information in the blockchain or sends it to a remote Namecoin server that does the look up for him. Domain names ending with any other extension will be forwarded to a DNS resolver that will resolve the domain name and respond with the answer.

The danger in using this approach is that the DNS might not be decommissioned, leaving the Internet with two systems working in parallel for a very long time. Because both systems work, there is no need for clients/resolvers to fully switch from one to another. This can also lead to inconsistencies, because domains need to be updated in both systems. At some point the decision must be made to stop using the DNS and only use Namecoin.

5.3. Namecoin

Namecoin has chosen for an approach in which both the DNS and Namecoin are used simultaneously. Standard DNS queries are sent to a resolver (could be both locally or on a remote server). The resolver looks at the last part of the domain name: domain names ending with ".bit" are looked up in the blockchain and other domain names are forwarded to a DNS resolver.

6. DNS Ecosystem

The DNS is just a naming protocol, but over the years a whole ecosystem has been built around it. There are organizations that control the root of the DNS, companies that make money selling domain names to their customers and many more organizations that completely rely on the DNS.

A switch from the DNS to Namecoin could affect companies and possibly have huge implications on organizations like ICANN, IANA, SIDN and registrars. What will their role be in Namecoin and how can they anticipate on a possible switch.

In this section the roles that are existent in the DNS will be determined. A further explanation will elaborate the tasks that are performed by the roles. When the tasks are determined, the implications for every role will be discussed.

6.1. Roles

It is important to know which roles are currently existing in the DNS ecosystem. Based on these roles we can look at the implications for all of these roles. Together with SIDN Labs we created a list with all roles that are existent in the DNS. A short description has been added to it as well:

- Users: people that request domain names by sending queries to use the internet, generally using a resolver.
- Resolver operators: system administrators that set up and maintain a resolver to serve users. This is often arranged by an ISP or the IT department of a company.

- Name server operators: system administrators that set up and maintain name servers that are authoritative for a single or multiple domain(s) and answer queries accordingly.
- Registrants: someone that registers a domain name (possibly by using a registrar).
- Registrar: a company that allows registrants to register a domain name (and often charges money for it).
- Registry: organizations that hold a database of all domain names and associated registrant information. Examples are ICANN/IANA and SIDN. As part of their activities they act as name server operator as well.

6.1.1. Users

The users of the DNS are the people that try to access certain domain names. Most users do not have any knowledge of the DNS and do not even know that such a system exists. They just expect it to work (when they try to access a website for instance). The users generally use client applications that access the DNS stub resolver that is built into the operating system to resolve DNS queries. A stub resolver is not capable of performing the complete lookup process and will ask a resolver to do the lookup for him.

6.1.2. Resolver Operators

Resolver operators are system administrators that offer resolvers to their users/customers. Their task is to offer name servers that will query authoritative name servers and follow referrals on behalf of the client. Because most users have no knowledge of the DNS, most ISPs and IT departments offer DNS resolvers as part of their standard services. There are also public resolvers available that are offered by other parties like OpenDNS, OpenNIC and Google.

6.1.3. Name Server Operators

Name server operators are system administrators that offer authoritative name servers. This enables resolvers to look up domain names. Every domain needs authoritative name servers that can respond to queries destined for that domain or one of its sub-domains. Many registrars offer name servers for their customers as an extra service, but many registrants run their own name servers as well to get more control over their domain.

6.1.4. Registrants

Registrants are people that register a domain name. They often pay a registrar to register the domain for them. By registering a domain name they are able set up a website, get a personalized e-mail address, etc. All registrants have to provide data to a name server that is authoritative over the registered domain. Most registrars offer those name server so registrants do not have to administer their own name server.

6.1.5. Registrars

Registrars are companies that allow their customers to buy domain names. They make sure that a domain gets registered and the registrant information is made available to the registry. Many registrars offer extra services to their customers, making them name server operators as well.

6.1.6. Registries

The registry is an organization that registers who owns which domain names. They keep data like the name of the person/company, and contact information. Organizations like ICANN, IANA and SIDN are examples of registries. For every top-level domain there is an associated registry. Some registrants are a registry as well by selling sub-domains of their own domains to others (an examples could be **.fami.ly*). Registries are name server operators as well because they need to delegate the authority of their sub-domains to the registrants (IANA administers there root name servers and SIDN administers the .nl domain). Some TLDs have chosen to outsource (parts of) their operations as well.

6.2. Implications

Changing from the DNS to Namecoin can have huge effects on all roles that are currently existent in the DNS. The switch could effect these roles by changing the way they currently operate, but some roles will become needless. In this section the implication for every role will be discussed independently, assuming that Namecoin would completely take over the DNS.

6.2.1. Users

As told in section 6.1.1 most users do not have any knowledge of the DNS. Applications make use of the client stub which makes recursive queries to the configured resolver. When the switch to Namecoin will be made, most users will not notice any changes. The only thing that might be noticed is the new TLD that ends with .bit.

The users are still not aware of the underlying naming system. Applications will make use the client stub to resolve domain names. However, the client stub that is built into the operating system does have to change. Where it is currently configured to forward queries to a name server, there are now two options: the client stub becomes a resolver that is able to look up domain names in the blockchain or it forwards queries to a name server that will look up the domain in the blockchain.

The first option requires the blockchain to be stored locally and the client stub to evolve in a full resolver. The second option allows the stub resolver to forward requests to a remote server. The benefits and downsides of both choices have been discussed in section 4.2.

6.2.2. Resolver Operators

Resolver operators make name servers available that will perform domain lookups for client stubs that are not able to resolve domain names them selves. When the blockchain is locally available, there is no need to forward requests to a remote resolver because the client took over this functionality. However, if the client for whatever reason is not able or does not want to store the blockchain locally, it needs to forward the queries to a resolver that does have the blockchain locally available.

In other words, resolver operators will stay available for clients that do not store the blockchain locally. Because Namecoin is very different from the DNS it is important that resolver operators gain knowledge of Namecoin and the possible related protocols. This way they are able to successfully operate a resolver.

6.2.3. Name Server Operators

DNS stores resource records at servers that are authoritative over certain domain names. Namecoin takes a different approach by distributing the resource records to all clients. Dedicated servers that serve answers to queries of specific domains do not exist in Namecoin. All clients with a local blockchain have the data of all domains available.

The name server operators / registrants do not have to operate dedicated servers containing DNS data any more. Instead they only need to maintain the data of their domain(s) which is stored in the blockchain. This can be done using client applications like Namecoin-Qt or namecoind.

6.2.4. Registrants

Registrants will notice differences as well. Using the DNS, registrants are required to register domain names through registrars. The registrars register the domain at the registry and communicate back to the registrant. In Namecoin a registrant can simply download an application and register domains using that application.

Most registrars also charge money for registering domain names, often in the range of €5 - €20 per year. In Namecoin the registration of domain names will cost just 0.01 NMC per domain, currently worth roughly €0.0038. This is excluding the transaction fee of 0.005 NMC per transaction.

6.2.5. Registrars

As told in section 6.2.4 registrars are not necessary to register domain names in Namecoin. Registrants can buy Namecoins and register a domain name using a client application.

Although it sounds pretty easy, some registrants might not be able to understand this or do not want to be bothered with the hassle. Especially gaining Namecoins can be expensive or difficult. A registrar could register a domain name for the registrant asking a small fee in return (using any currency), taking away the hassle of buying Namecoins and registering the domain names for registrants.

6.2.6. Registries

Like registrars, registries are needless as well because registrants can register domains directly without any organization in between. Due to the design of Namecoin, registries are not needed to register data about the registrants, this information can be stored in the blockchain itself and a registrant can choose to do this or not.

In DNS there are registrants that are registries as well because they sell sub-domains of their own domain. This is also possible in Namecoin. A registrant can delegate authority of a sub-domain to another domain, possibly after accepting payments (in any desired currency).

6.3. New Roles

Although a switch to Namecoin may have implications on the roles that currently exist in the DNS, there are also new opportunities that arise. This section discusses some of new roles in Namecoin.

6.3.1. Mining

Mining, as explained in section 2.3, is the process that secures Namecoin from fraudulent transactions. On average every 10 minutes a miner node in the network mines a block of transactions. The miner that mines this block receives an award for it and keeps the transaction fee that is associated with the transactions in that block.

The mining fee started with 50 NMC and decreases by 50% every 210.000 blocks. Currently the mining fee is 25 NMC which is worth roughly €9.60. Although the value of Namecoins is currently not that high, it might be the case that the value will increase in the upcoming years, just like Bitcoin did from 2013 [18]. The difficulty of mining Namecoins is not nearly as high as mining Bitcoins, meaning less expensive equipment is needed to be successful.

Merged Mining
Namecoin also allows merged mining. In merged mining one can calculate hashes over Bitcoin blocks, but is still able to receive Namecoins for it. If a Bitcoin hash meets the difficulty of Namecoin (and possibly the difficulty of Bitcoin as well), the Bitcoin block will be accepted as proof of work for Namecoin.

By adding the Bitcoin block header, the corresponding hash and all Bitcoin transactions, one can proof it has done the required work to meet the difficulty and thereby Namecoin will accept the mined block. This way it is possible to mine both Namecoin and Bitcoin blocks at the same time without increasing computing power. [19]

Mining Pools
In mining pools many miners bundle their compute power together to mine blocks. Mining pools increase the chance of mining blocks because the miners can simultaneously work on different nonces to solve a block.

When a block has been mined, the rewards will be shared amongst all miners in the pool based on the amount of compute power that is brought to the pool. There are mining pools for Bitcoin, Namecoin, and many more Bitcoin alike systems, but also pools that support merged mining.

6.3.2. Namecoin Exchanges

Registering domain names will cost a small amount of Namecoins. Those Namecoins can be earned by mining, but depending on the compute power one has available it can take days, weeks or even years before a block has been mined. People that successfully mined Namecoins or retrieved Namecoins in another way, also sell the Namecoins they do not use.

After a while currency exchanges started trading Namecoins for other currencies in return for a small fee. They now buy and sell Namecoins for Bitcoins, euros, dollars, and many other currencies. For users that want to start using Namecoin, this is the easiest way to obtain Namecoins.

6.3.3. Online Wallets

The public and private keys of Namecoin wallets need to be stored very carefully. Loosing a wallet means that all Namecoins related to that wallet are inaccessible and data registered in the blockchain (like domain names or identities) cannot be changed any more. Proper backups are important to make sure keys are not lost, but some people do not trust themselves in doing so. Therefore they would like others to do that for them.

Due to this demand some websites offer services to maintain wallets online. They can create wallets for Namecoin users and make sure the wallets are properly stored and backed up. Some Namecoin exchanges also offer this as an extra service.

The danger in these online wallets is that one needs to trust the website offering the wallets. The websites own the wallets containing the private keys, theoretically making it possible for them to make transactions with it. All Namecoins and registered data associated with those wallets are in their hands.

7. Conclusion

How does Namecoin work?
Namecoin is very similar to Bitcoin. All the functionality that can be found in Bitcoin is available in Namecoin. In addition to Bitcoin it is not only possible to transfer the currency from one person to another, but also to store data in the blockchain. Data is identified by an application specifier that specifies what type of data is stored within a certain record. Domains are made available under the .bit TLD and need to use the same syntax as stated in RFC 1035. The resource records are stored using JSON objects with a maximum size of 520 bytes.

Domains are valid for 36.000 block, corresponding to roughly 200-250 days.

What are the current shortcomings of the DNS system?
In RFC 3833 a few well-known attacks against the DNS are described to determine if DNSSEC was meeting its design goals. The following attacks were mentioned: packet interception, ID guessing & query prediction, name chaining, betrayal by trusted servers, authenticated denial of domain names, denial of service and wildcard matching.

Because of the decentralized design, the DNS is vulnerable for censorship by organisations with much power. The DNS is also not offering any encryption by default, meaning that privacy cannot be assured.

Which of the shortcomings of the DNS does Namecoin address?
Depending of the usage of Namecoin, all of the attacks described in RFC 3833 can be addressed. When the blockchain is stored locally it addresses all attacks. However, when the blockchain is stored on a remote machine, clients need to switch back to the original DNS protocol. This makes the packet interception, ID guessing & query prediction, betrayal by trusted servers, denial of service and wildcard matching attacks possible again. The authenticated denial of domain names cannot be trusted any more.

Censorship-resistance can be offered due to the distributed design of Namecoin. All nodes are equal to each other. Privacy can be assured when the blockchain is stored locally because there are no plain text queries that need to go over the internet. Namecoin claims to be faster as well but this has not been verified.

Can Namecoin match the robustness of the DNS?
The DNS is a decentralized system in which a hierarchical structure is used. Much load is put on the root name servers (the top of the tree) and further down in the tree less resources are needed.

Namecoin is a distributed system, this will distribute all the load (queries, registrations and data distribution) over all nodes in its network. This P2P system ensures that all nodes only need few resources instead of few servers that need many resources.

What are the consequences for the different organisational roles?
There are a number of roles in the DNS, there are users, resolver operators, name server operators, registrants, registrars and registries. The users and registrants will not notice much of the changes. It will stay just as easy to access a domain name and the registration of domain names can be done by the registrant itself. Resolver operators and registrars are not necessary, but probably they will stay available in Namecoin because not every node is able to store the full blockchain and not all registrants are capable of registering domain names or retrieving Namecoins. Name server operators and registries are needless in the Namecoin system.

How would a transition scenario from the DNS to Namecoin look like?
A transition in Namecoin would happen in two phases. During the first phase all domain names need to be made available in Namecoin. In the seconds phase the clients need to be able to resolve Namecoin domains.

In the first phase one retrieves Namecoins and registers a domain by using a client application. The second phase can be accomplished in two different scenarios. In the first scenario one determines a specific date or time frame in which the switch from the DNS to Namecoin is made. In the second scenario the Namecoin and DNS queries will be resolved in parallel. Based on the TLD (.bit) a domain can be looked up in the blockchain or in the DNS.

8. Future Work

Namecoin definitely looks promising, but there is much that needs to be improved before it can be used on the Internet.

The blockchain is going to contain a lot of data when it is used more actively, making it hard to store it locally. In the case that the blockchain needs to be stored on a remote server it will fall back to traditional DNS queries that are vulnerable for the attacks described in 4.1.

To defend against all the listed attacks and offer the privacy that Namecoin can offer when a local blockchain is available, the DNS protocol needs to be replaced by another protocol. Possibly one could make use of existing protocols like DNSCurve to encrypt the traffic and ensure packets cannot be replayed. However, maybe there are even better solutions like designing a complete new protocol for remote access.

As an addition to the storage problem, it might be beneficial for some clients to store only the latest 36.000 blocks. Currently the whole blockchain is stored to ensure the integrity of the data. This includes transactions that have been expired. By storing only the last 36.000 blocks, only non-expired transactions are saved, reducing the size of the blockchain considerably (to an estimate of 512 MiB).

Clients that are not able to store the full blockchain might be able to store a light-weight variant of the blockchain. However, storing only part of the blockchain might have consequences for the integrity of the data in the blockchain. Researching this possibility could make it easier to adopt Namecoin, provided that the integrity can still be ensured.

Another thing that has not been researched is the performance of Namecoin compared to the DNS. We believe it is plausible that lookups in Namecoin are significantly faster than lookups in the DNS. Especially when the blockchain is stored at the client and the queries do not have to go over the Internet.

Until proper measurements are done we cannot be sure if our expectations are actually true. There are many things that need to be taken into account (think of the size of the blockchain, caching, lookup algorithms and processing power), making it possible to dedicate a complete project to the performance comparison.

Acknowledgements

I would like to thank SIDN Labs a lot for providing this project and the supervisor. In particular Marco Davids, his help during the project has been really valuable for me. Furthermore I would like to the University of Amsterdam for providing the workspace, facilities and opportunity to do this research.

References

[1] Jacobs, F. (2014). Providing better confidentiality and authentication on the Internet using Namecoin and MinimaLT (arXiv:1407.6453v1). Accessed from http://arxiv.org/abs/1407.6453

[2] Melin, T., & Vidhall, T. (2014). Namecoin as authentication for public-key cryptography (LIU-IDA/LITH-EX-G–14/067–SE). Accessed from http://liu.diva-portal.org/smash/record.jsf?pid=diva2%3A730344&dswid=-2203

[3] Atkins, D. and Austein, R. (2004). RFC 3833 - Threat Analysis of the Domain Name System (DNS). [online] Tools.ietf.org. Available at: https://tools.ietf.org/html/rfc3833 [Accessed 7 Jan. 2016].

[4] Wiki.namecoin.info, (n.d.). Namecoin Wiki - FAQ. [online] Available at: https://wiki.namecoin.info/index.php?title=FAQ [Accessed 13 Jan. 2016].

[5] Antonopoulos, A. (2014). Mastering Bitcoin. Sebastopol, California: O'Reilly.

[6] Weaver, N., Kreibich, C., Nechaev, B. and Paxson, V. (2002). Implications of Netalyzrs DNS Measurements. [online] The ICSI Networking and Security Group. Available at: http://www.icir.org/christian/publications/2011-satin-netalyzr.pdf [Accessed 29 Jan. 2016].

[7] Wilcox-O'Hearn, Z. (2006). Names: Decentralized, Secure, Human-Meaningful: Choose Two. [online] Shoestringfoundation.org. Available at: http://shoestringfoundation.org/ bauerm/names/distnames.html [Accessed 18 Jan. 2016].

[8] Cohen, B. (2015). What is Onename?. [online] Onename. Available at: https://onename.zendesk.com/hc/en-us/articles/202288932-What-is-Onename- [Accessed 14 Jan. 2016].

[9] Cheshire, S. and Krochmal, M. (2013). RFC 6761 - Special-Use Domain Names. [online] Tools.ietf.org. Available at: https://tools.ietf.org/html/rfc6761 [Accessed 28 Jan. 2016].

[10] Grothoff, C., Wachs, M., Wolf, H., Appelbaum, J. and Ryge, L. (2015). Draft: Special-Use Domain Names of Peer-to-Peer Systems. [online] Internet Engineering Task Force. Available at: https://www.ietf.org/archive/id/draft-grothoff-iesg-special-use-p2p-names-04.txt [Accessed 28 Jan. 2016].

[11] Grothoff, C., Wachs, M., Wolf, H., Appelbaum, J. and Ryge, L. (2015). Special-Use Domain Name for Namecoin. [online] Ietf.org. Available at: https://www.ietf.org/archive/id/draft-grothoff-iesg-special-use-p2p-bit-00.txt [Accessed 28 Jan. 2016].

[12] Mockapetris, P. (1987). RFC 1035 - Domain names - implementation and specification. [online] Tools.ietf.org. Available at: http://tools.ietf.org/html/rfc1035 [Accessed 15 Jan. 2016].

[13] Wiki.namecoin.info, (n.d.). Domain Name Specification - Namecoin Wiki. [online] Available at: https://wiki.namecoin.info/index.php?title=Domain_Name_Specification [Accessed 15 Jan. 2016].

[14] rootops, (2015). Events of 2015-11-30. [online] Root-servers.org. Available at: http://root-servers.org/news/events-of-20151130.txt [Accessed 15 Jan. 2016].

[15] Calpito, D. (2015). Hacktivist Group Anonymous Declares War Against Turkey, Takes Down 400,000 Sites. [online] Tech Times. Available at: http://www.techtimes.com/articles/119815/2015 1229/hackitivist-group-anonymous-declares-war-against-turkey-takes-down-400-000-sites.htm [Accessed 15 Jan. 2016].

[16] Pieters, J. (2015). Telecom Ziggo struck in second cyber attack this week - NL Times. [online] NL Times. Available at: http://www.nltimes.nl/2015/08/20/telecom-ziggo-struck-in-second-cyber-attack-this-week/ [Accessed 16 Jan. 2016].

[17] Mockapetris, P. (1987). RFC 1034: DOMAIN NAMES - CONCEPTS AND FACILITIES. [online] Ietf.org. Available at: https://www.ietf.org/rfc/rfc1034.txt [Accessed 15 Jan. 2016].

[18] Higgins, S., Ross, R., Palmer, D., Rizzo, P., Wong, J. and Rizzo, P. (2016). Bitcoin Price Index - Real-time Bitcoin Price Charts. [online] CoinDesk. Available at: http://www.coindesk.com/price/ [Accessed 21 Jan. 2016].

[19] Schwartz, D. (2011). How does merged mining work?. [online] Bitcoin.stackexchange.com. Available at: https://bitcoin.stackexchange.com/questions/273/how-does-merged-mining-work [Accessed 21 Jan. 2016].

Appendices

A. Domain Name Entries in Namecoin

These are all possible domain name entries that can be used within Namecoin including the DNS resource record type equivalent. An updated list can be found at the wiki page from wiki.namecoin.info [13]

Entry type	DNS equivalent	Description
ip	A	IPv4 addresses.
ip6	AAAA	IPv6 addresses.
tor	n/a	Tor hidden service address.
i2p	n/a	Eepsite information. At least one hint is required.
freenet	n/a	Freesite Key.
service	SRV	Used to identify hosts that support particular services as per DNS SRV records.
alias	CNAME	Specifies that this name is an alias of the given string, which can either be one of the sub-domain names in context or an absolute domain name. Absolute domain names are signified by an added dot (.) in the end.
translate	DNAME	translate Specifies that all subdomains of this name are translated to the given String before lookup. As with alias, absolute domain names end with a dot (.).
email	SOA or RP	Hostmaster e-mail address.
loc	LOC	Geographic location information.
info	n/a	A JSON value reserved for registrant information.
ns	NS	Array of master nameservers of the configured domain, which can be either IPs or absolute domain names. Note that this delegates all IP related responsibility of this domain and its sub-domains to the master server, effectively bypassing other settings (e.g. ip).
delegate	n/a	Delegates control of this domain to the given Namecoin name, or a sub-domain entry defined within that name. All other entries are ignored.
import	n/a	Imports specified entries from Namecoin names and merges with the current one.
map	n/a	Maps sub-domains to their respective configurations.
fingerprint	n/a	Depricated: Specifies one or more certificate fingerprint(s). Is now replaced by “tls”
tls	n/a	Specifies one or more certificate fingerprints for specific protocols and ports. Attempts to follow the DANE protocol closely. Adds includeSubdomains.
ds	DS	DNSSEC fingerprints for securing the domain when used with DNS via ns. Format roughly mirrors RFC3658 - the fields are keytag, algorithm, hash type, and base64(hash(domain + DNSKEY RRDATA)).