# **Identity**

# **1 Basics**

A table with an overview of the support status and applicability.

|  |  |
| --- | --- |
| Status: | e.g. **Supported**/**Tech Preview**/**Experimental** |
| Architecture(s): | e.g. x86, arm |
| Component(s): | e.g. Hypervisor, toolstack, guest |
| Hardware: | *where applicable* |

# **2 Overview**

Cryptocurrency blockchains and their respective P2P networks are useful beyond exchanging money. They provide cryptographically auditable, append-only ledgers that are already being used to build new, decentralized versions of DNS and public-key infrastructure, along with other applications like file storage and document timestamping. Because blockchains have no central points of trust or failure, they enable a new class of decentralized applications and services that minimize the degree to which users need to put trust in a single party, like a DNS root server or a root certificate authority. Blockchain networks have attracted a lot of interest from enthusiasts, engineers, and investors. In fact, 1.1 billion USD has been invested in blockchain startups over the last several years. With the rapid capital infusion, infrastructure for blockchains is getting quickly deployed, and blockchains are emerging as publicly available common infrastructure for building decentralized systems and applications. However, blockchain networks are at a very early stage, and there is very little production data available to guide design trade-offs. Many non-financial applications of blockchains imply the need for a naming system that securely binds names, which can be human-readable, to arbitrary values. The blockchain gives consensus on the global state of the naming system and provides an append-only global log for state changes. Writes to name-value pairs can only be announced in new blocks, as appends to the global log. The global log is logically centralized (all nodes on the network see the same state), but organizationally decentralized (no central party controls the log). The decentralized nature of blockchain-based naming introduces meaningful security benefits, but certain aspects of contemporary blockchains present technical limitations. Individual blockchain records are typically on the order of kilobytes and cannot hold much data. The latency of creating and updating records is capped by the blockchain’s write propagation and leader election protocol, and it is typically on the order of 10-40 minutes. The total new operations in each round are limited by the average bandwidth of nodes participating in the network (for Bitcoin the current average is ∼1500 new operations per new round). Further, new nodes need to independently audit the global log from the beginning: as the system makes forward progress, the time to bootstrap new nodes increases linearly.

# **3 User details**

Just like DNS, there is a cost associated with registering a new name. The name registration fee discourages people from registering a lot of names that they don’t intend to use. In Namecoin, the recipient of registration fees is a “black hole” cryptographic address from which money cannot be retrieved. Namecoin defines a pricing function for how the cost of name registrations changes over time. Namecoin supports multiple namespaces (like TLDs in DNS), and the same rules for pricing and name expiration apply to all namespaces. By convention, the d/ namespace is used for domain names. In Namecoin, name registration uses a two-phase commit method where a user first pre-orders a name hash and then registers the name-value pair by revealing the actual name and the associated value. This is done to avoid front-running of unconfirmed name registrations. Name registrations to expire after a fixed amount of time, measured in new blocks written (currently 36,000 blocks, which translates to roughly eight months). Namecoin also supports updating the value associated with a name, as well as ownership transfers.

# **4 Technical details**

Information for a developer or power user. Should include where to look in-tree for detailed documents and code.

# **5 Limitations**

The security of name ownership is tied to the security of both the underlying blockchain and the software powering it. The most important factor in the security of a blockchain is the total cost of attacking the blockchain and tampering with recently written data. Miners often pool their resources to form a mining pool, which is essentially a super node on the network (a lot of computational power behind a single miner node). If the amount of computational power under the control of a single miner (or pool) is more than the rest of the network, called a 51% attack, then that miner has the ability to attack the network and rewrite recent blockchain history, censor transactions (e.g., for name registrations), and steal cryptocurrency using double spend attacks. This is because it will win the leader election for a majority of the time, and produce a blockchain history with more proof-of-work than any disagreeing miner. The more expensive it is to control a majority of the compute power on a blockchain, the more secure the blockchain. We noticed in late 2014 that a single mining pool consistently had more than 51% of the compute power on Namecoin. Recently, the situation has been even worse, with a single mining pool controlling over 60% of Namecoin’s compute power. Figure 1 shows the weekly and daily distribution of mining power for the month of August 2015, right before we migrated our system away from Namecoin. In fact, we have observed F2Pool (also known as Discus Fish) control up to 75% of compute power in a particular week. At such concentration, Namecoin is effectively controlled by a single party; F2Pool gets to write most of the new blocks and can undermine the security of the blockchain at will. Other than raw hashing power, software bugs can also introduce security problems, e.g., a Namecoin bug allowed people to steal names from anyone [26]. Denial-of-service attacks are another attack vector; the more peers a cryptocurrency network has, the more resilient the network is to denial-of-service attacks. Bitcoin currently has the largest amount of computational power securing the blockchain data. Bitcoin’s codebase is more actively developed with more bug bounties than other blockchains. Namecoin has many fewer peer nodes than Bitcoin (170 vs. 4,600 in Jan 2016), which makes it more vulnerable to DDoS attacks as well. The Bitcoin blockchain is currently by far the most secure blockchain. However, it’s extremely hard to introduce new functionality to Bitcoin because that requires consensus-breaking changes.

# **6 Testing**

Information concerning how to properly test changes affecting this feature.

# **7 Areas for improvement**

List of enhancements which could be undertaken, e.g. to improve the feature itself, or improve interaction with other features.

# **8 Known issues**

List of known issues or bugs. For tech preview or experimental features, this section must contain the list of items needing fixing for its status to be upgraded.

# **9 References**

Relevant external references for this feature.