Namecoin

Namecoin

- Similar to DNS

- Allows anyone to register a name

- Decentralized, no trusted third party

- First fork of Bitcoin!

Namecoin

- Extension to Bitcoin script with 3 new opcodes
  - NAME_NEW
  - NAME_FIRST_UPDATE
  - NAME_UPDATE

Namecoin

- Extension to Bitcoin script with 3 new opcodes
  - NAME_NEW
  - NAME_FIRST_UPDATE
  - NAME_UPDATE

NAME_NEW: Hash(random_nonce, "agervais")

Time

Namecoin

- Extension to Bitcoin script with 3 new opcodes
  - NAME_NEW
  - NAME_FIRST_UPDATE
  - NAME_UPDATE

NAME_NEW: Hash(random_nonce, "agervais")

NAME_FIRST_UPDATE: random_nonce, "agervais", {"ip":"234.22.34.23"}

Time

Namecoin

- Extension to Bitcoin script with 3 new opcodes
  - NAME_NEW
  - NAME_FIRST_UPDATE
  - NAME_UPDATE

NAME_NEW: Hash(random_nonce, "agervais")

NAME_FIRST_UPDATE: random_nonce, "agervais", {"ip":"234.22.34.23"}

NAME_UPDATE: random_nonce, "agervais", {"ip":"234.22.34.24"}

Time

Namecoin

- Extension to Bitcoin script with 3 new opcodes
  - NAME_NEW
  - NAME_FIRST_UPDATE
  - NAME_UPDATE

NAME_NEW: Hash(random_nonce, "agervais")

Is there something to consider?

NAME_FIRST_UPDATE: random_nonce, "agervais", {"ip":"234.22.34.23"}

NAME_UPDATE: random_nonce, "agervais", {"ip":"234.22.34.24"}

Time

Namecoin

- Extension to Bitcoin script with 3 new opcodes
  - NAME_NEW
  - NAME_FIRST_UPDATE
  - NAME_UPDATE

NAME_NEW: Hash(random_nonce, "agervais")

Is there something to consider?

Wait for 12 blocks,
preventing frontrunning!

NAME_FIRST_UPDATE: random_nonce, "agervais", {"ip":"234.22.34.23"}

NAME_UPDATE: random_nonce, "agervais", {"ip":"234.22.34.24"}

Time

Namecoin Fees

Register a domain with namecoin

How much does it cost

You can register a .bit domain by buying it with namecoins with the namecoin software. You will be your own registrar by using the namecoin software. The fee consists of two parts: the registration fee plus the transaction fee (as for every transaction).

Command	Registration Cost	Fees	Summary	Notes
name_new	0.01NMC	Standard*	pre-order a domain, fixed cost	You still don't own the domain!
name_firstupdate	0NMC (Price Calculator)	Standard*	register a domain, it becomes public, variable cost	You own the domain!
name_update	0.00NMC	Standard*	domain is updated, transfered or renewed	Reset the expire time to the max

* Standard fees are 0.005NMC (same rules as bitcoin for tx with no fees). ## 1. Install the namecoin software [Install and configure namecoin](https://github.com/namecoin/namecoin/wiki/Install-and-Configure-Namecoin)

2. Pre-order a domain name

is your domain without .bit, in lowercase. For internationalized domain names, the IDNA ASCII standard is used, and direct Unicode entries are not supported. Use this online tool to check and convert your domain : http://dot-bit.org/tools/domainSearch.php Or check if your domain if free with the command line (the command line don't do the conversion) :
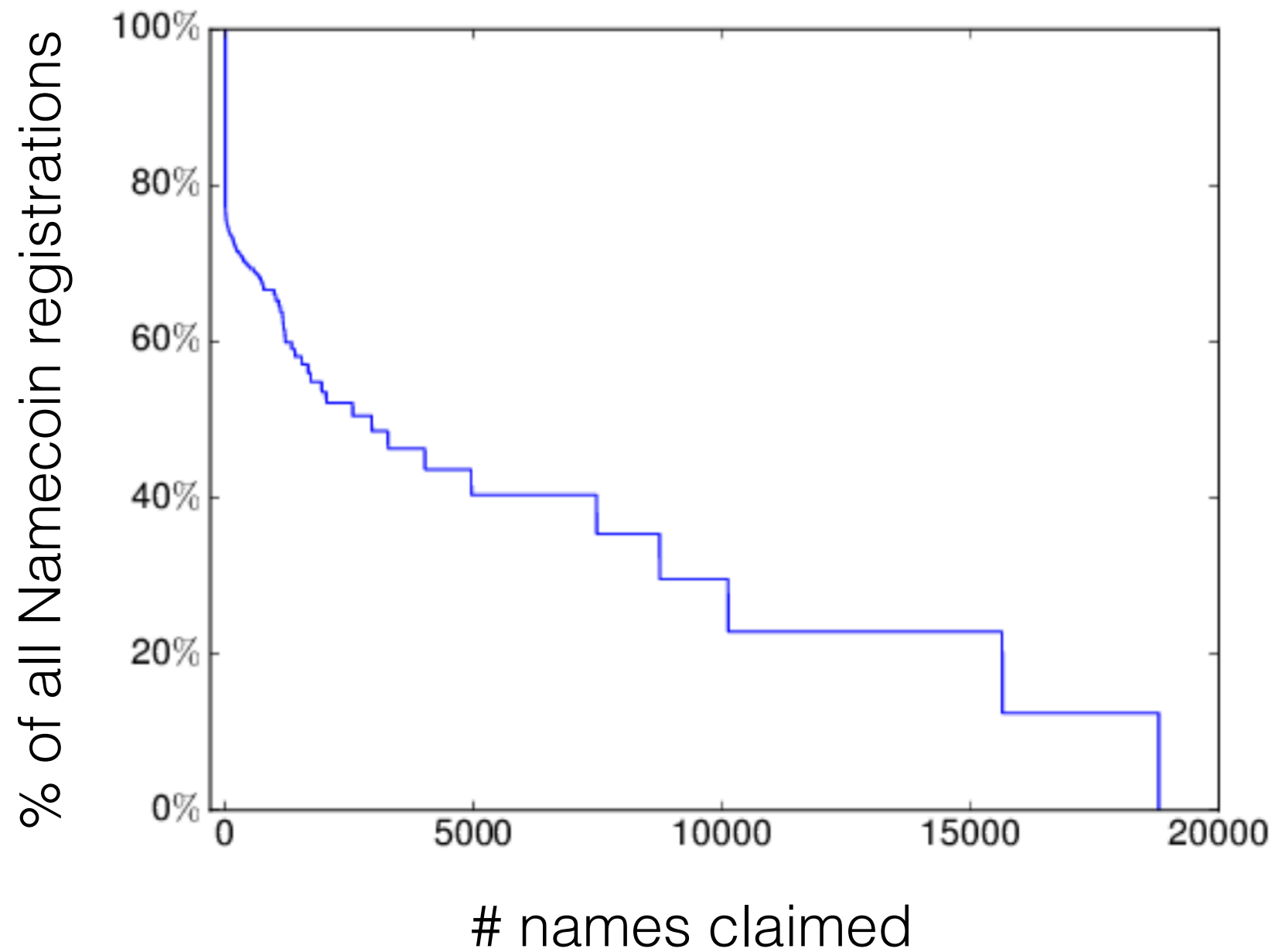
    ./namecoind name_new d/

Start the namecoin software and use the following command :
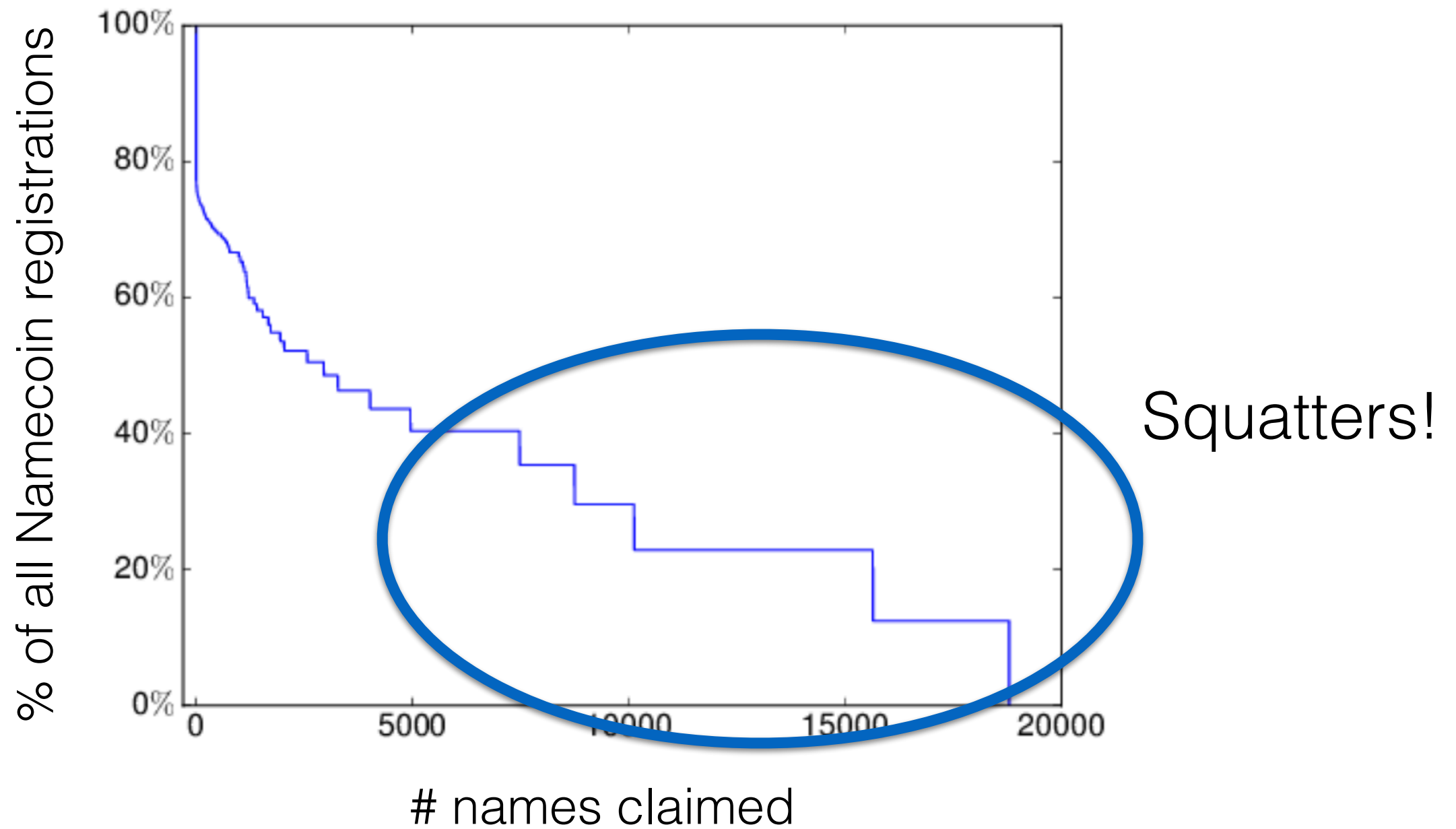
    ./namecoind name_new d/

The output will looks like this :

Namecoin's Bad Incentive Structure

An empirical study of Namecoin and lessons for decentralized namespace design, Kalodner et al., WEIS 2015

Namecoin's Bad Incentive Structure

Squatters!

An empirical study of Namecoin and lessons for decentralized namespace design, Kalodner et al., WEIS 2015

New Functionality for Bitcoin

new addition	Purpose	In Namecoin	In OpenBazaar/ Futurecoin
Global State	Track application data	Register name	merchants, ask and bid
Opcodes	Write to global state	NAME_NEW, etc.	OPEN_MARKET, etc.
Fees	Limit spam, computation and storage read/write	Registration fee to limit squatting, expiry	Transaction fees for trades

New Functionality for Bitcoin

new addition	Purpose	In Bitcoin
Global State	Track application data	**UTXO set**
Opcodes	Write to global state	**Transactions**
Fees	Limit spam, computation and storage read/write	**Implicit with transaction fees**