Namecoin as an alternative to the DNS

Xander Lammertink

Research questions

- Can Namecoin be an alternative to the DNS?
  - How does it **work**?
  - What are the **shortcomings** of the DNS?
  - What are the **consequences**?
  - Can Namecoin match the **robustness** of the DNS?
  - How would a **transition** scenario look like?

Bitcoin

Bitcoin

- Wallets
- Transactions
- Mining
- Blockchain

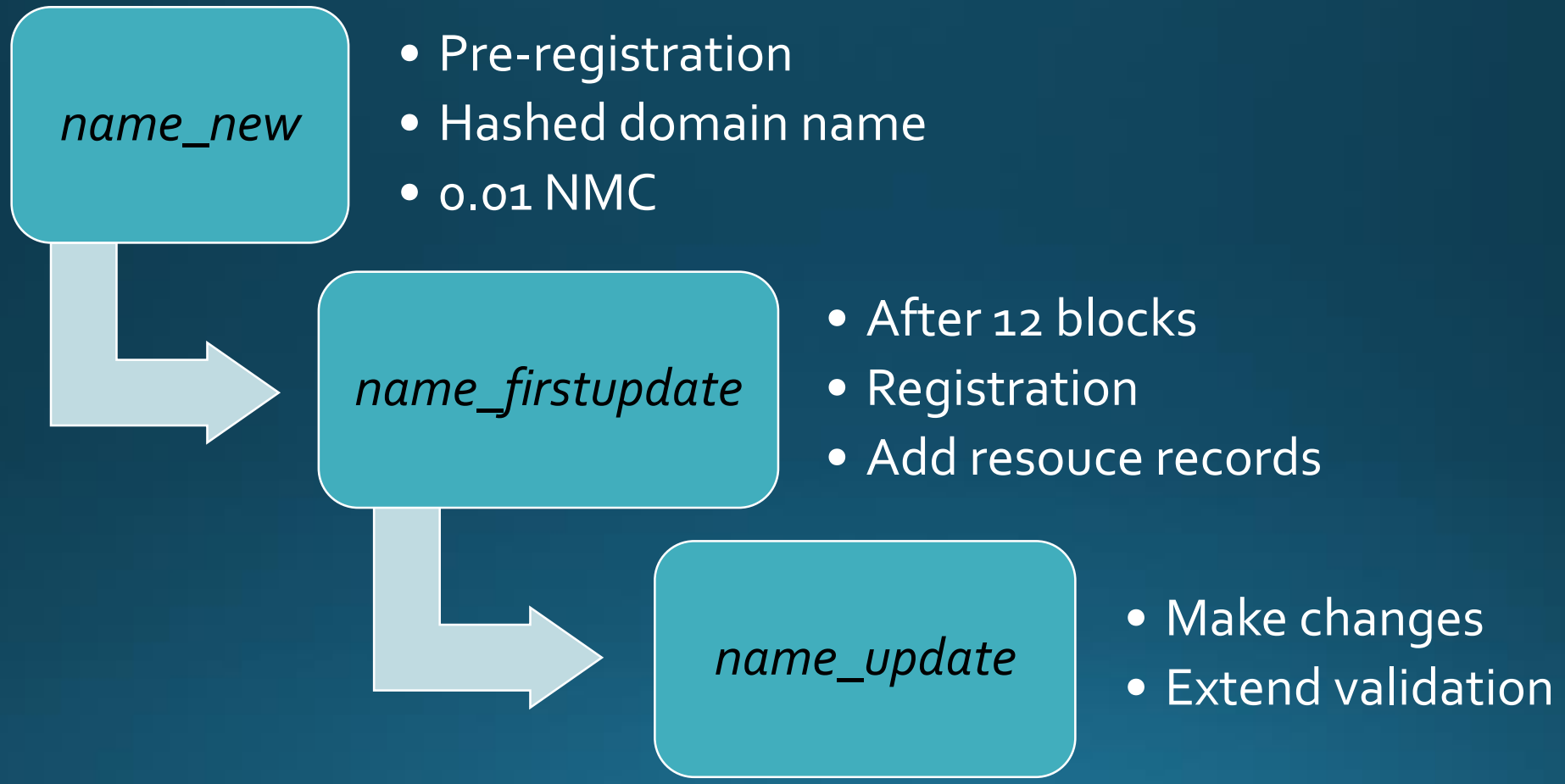
Namecoin

Features

- Domain names *d/*
- Identities *id/*

- OneName *u/* or *i/*
- Product metadata *p/*
- Proof of existence *poe/*

Registration



Domain Name System

RFC 3833

- Packet interception
- ID guessing & query prediction
- Name chaining
- Betrayal by trusted servers
- Authenticated denial of domain names
- Denial of service
- Wildcard matching

Locally stored blockchain

- Packet interception
- ID guessing & query prediction
- Name chaining
- Betrayal by trusted servers
- Authenticated denial of domain names
- Denial of service
- Wildcard matching

Remotely stored blockchain

- Packet interception
- ID guessing & query prediction
- Name chaining
- Betrayal by trusted servers
- Authenticated denial of domain names
- Denial of service
- Wildcard matching

Transition scenario

Domain names

- Retrieve Namecoins
- Register domain name

Resolving

- Hard switch
  - Decide date / timeframe
  - Switch
- Parallel
  - Add Namecoin resolving

DNS Ecosystem

Roles

- Users
- Resolver operators
- Name server operators
- Registrant
- Registrar
- Registry

Roles

- Users
- Resolver operators
- Name server operators
- Registrant
- Registrar
- Registry

New roles

- Mining
- Namecoin exchanges
- Online wallets

Conclusion

- DNS suffers from attacks
- Namecoin can defend against them
  - Very robust
  - Transition without noticing
- Some roles will change, some will disappear
  - User is better off

Future work

- Protocol between client and resolver
- Performance measurements
- Storing part of the blockchain

Questions