Namecoin: Dezentrale Namen in der Blockchain

Daniel Kraft

25. März 2015

Überblick

Die Quadratur des Dreiecks

Zooko's Dreieck

Wähle **zwei aus drei**:

- dezentralisiert
- sicher und eindeutig
- aussagekräftig

Zooko's Dreieck

Wähle **zwei aus drei**:

- dezentralisiert
- sicher und eindeutig
- aussagekräftig

DNS, DNSSEC **Sicher** und **aussagekräftig**, aber nicht dezentral (ICANN, Root-Zone).

Spitznamen, GNS **Dezentral** und **aussagekräftig**, aber nicht notwendig eindeutig oder sicher.

Krypto **Dezentral** und **sicher**, aber nicht aussagekräftig: 1MjDWd6HwriGZakSDAZkye4rw1T6iXXRDj, BM-GtQnWM3vcdorfqpKXsmfHQ4rVYPG5pKS, 3g2upl4pq6kufc4m.onion, ...

Lösungsansätze

BitDNS Diskussion in der Bitcoin-Community, auch mit Gavin Andresen und Satoshi Nakamoto.

Aaron Swartz “Squaring the Triangle”, 6. Jänner 2011

Namecoin Anfang 2011 von **vinced** als (erster) Fork von Bitcoin implementiert.

Die Namecoin-Blockchain

Grundprinzip

Wer zuerst kommt, mahlt zuerst!

Die Namecoin-Blockchain

Grundprinzip

Wer zuerst kommt, mahlt zuerst!

- Namen sind dem Besitzer über ein **Schlüsselpaar** zugeordnet.
- **Gültige Signatur** zum Transfer und Update nötig.
- **Gebühren** verhindern DoS, Namen können auslaufen.
- Timestamping über eine **Blockchain** (wie bei Bitcoin).
- **Merge-Mining** auf Vorschlag von Satoshi Nakamoto.

Die Namecoin-Blockchain

Grundprinzip

Wer zuerst kommt, mahlt zuerst!

- Namen sind dem Besitzer über ein **Schlüsselpaar** zugeordnet.
- **Gültige Signatur** zum Transfer und Update nötig.
- **Gebühren** verhindern DoS, Namen können auslaufen.
- Timestamping über eine **Blockchain** (wie bei Bitcoin).
- **Merge-Mining** auf Vorschlag von Satoshi Nakamoto.

Namen sind **global eindeutig** und **fälschungssicher**!

Anwendungen für Namecoin

.bit, ein dezentrales DNS

Namecoin kann klassische DNS Information speichern:

d/domob

```
{
  "ip":  "176.31.184.255",
  "ip6": "2001:41d0:52:100::63f",
  "tor": "wivfwn64tm3uaeig.onion",
  "map": {"*": ...}
}
```

.bit, ein dezentrales DNS

Namecoin kann klassische DNS Information speichern:

d/domob

```
{
  "ip":  "176.31.184.255",
  "ip6": "2001:41d0:52:100::63f",
  "tor": "wivfwn64tm3uaeig.onion",
  "map": {"*": ...}
}
```

...und noch mehr, wie zum Beispiel **Onion-Adressen** und Schutz vor Zensur!

TLS-Zertifikate

Certificate Authorities

Wem kann man noch vertrauen?

TLS-Zertifikate

Certificate Authorities

Wem kann man noch vertrauen?

DANE mit DNSSEC gibt Kontrolle an den Server-Betreiber, aber erzeugt neue Probleme.

In Namecoin:

```
{
  ...,
  "fingerprint": ["F3C7..DD1A"]
}
```

Auflösen von .bit Domains

Externe DNS-Server Einfach zum Testen, aber natürlich nicht sicher oder privat!

Lokaler DNS-Server Zum Beispiel in **NMControl** für system-weite Einstellung, wird überarbeitet.

FreeSpeechMe Firefox-Erweiterung fürs Browsen mit Support für Onion-Seiten und TLS-Zertifikate.

Online-Identitäten

Dezentrale “Online-Profile”:

id/domob

```
{
  "name":       "Daniel Kraft",
  "email":      "d@domob.eu",
  "website":    "http://www.domob.eu/",
  "bitcoin":    "1domobKsPZ5cWk2kXssD8p8ES1qffGUCm",
  "bitmessage": "BM-GtQnWM3vcdorfqpKXsmfHQ4rVYPG5pKS",
  "gpg": ...,
}
```

Online-Identitäten

Dezentrale “Online-Profile”:

id/domob

```
{
  "name":       "Daniel Kraft",
  "email":      "d@domob.eu",
  "website":    "http://www.domob.eu/",
  "bitcoin":    "1domobKsPZ5cWk2kXssD8p8ES1qffGUCm",
  "bitmessage": "BM-GtQnWM3vcdorfqpKXsmfHQ4rVYPG5pKS",
  "gpg": ...,
}
```

→ Gut geeignet zum Tausch von öffentlichen Schlüsseln!

Ziel: “Send-to-ID”

NameID

- Passwort-loses Login
- Digitale Signatur einer Challenge
- Ein “Account” für viele Services
- Cold- und Hot-Wallets möglich
- OpenID-Provider und Bibliothek

Andere Ideen

Torrent-Verzeichnis TPB dezentral — Blockchain nötig?

Web-of-Trust Basierend auf Identitäten und Signaturen. Bewertungssystem?

Datei-Signaturen Hash der Datei als Name, Signatur als Wert.

Demonstration