



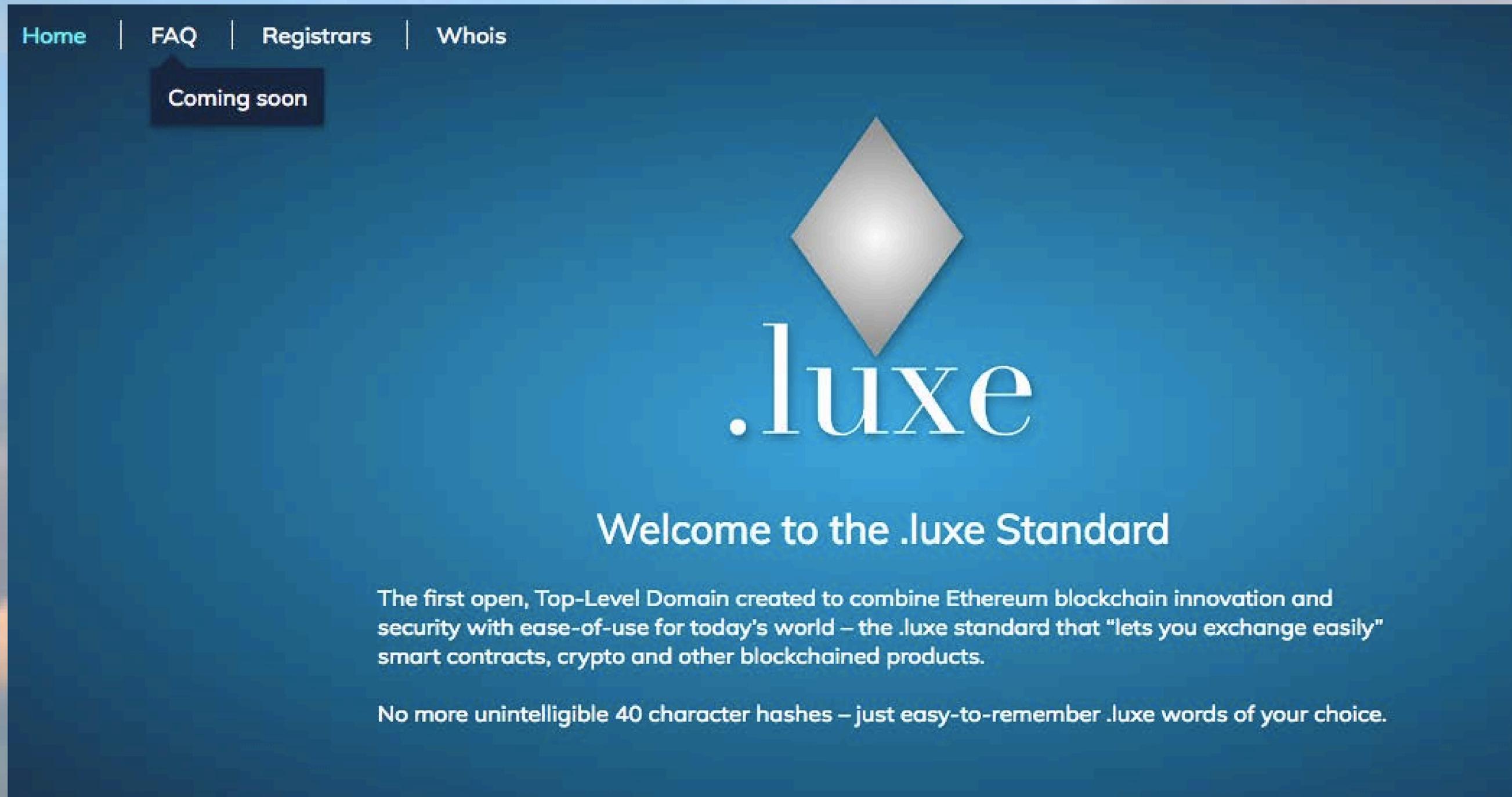
Blockchain и DNS

Воспоминание о будущем

Павел Храмцов
p.khramtsov@msk-ix.ru

TLDCON-2018
RIGA

Не верь глазам своим



Home | FAQ | Registrars | Whois

Coming soon

.luxе

Welcome to the .luxе Standard

The first open, Top-Level Domain created to combine Ethereum blockchain innovation and security with ease-of-use for today's world – the .luxе standard that "lets you exchange easily" smart contracts, crypto and other blockchained products.

No more unintelligible 40 character hashes – just easy-to-remember .luxе words of your choice.

The screenshot shows the ICANN website homepage. At the top, there is a dark blue navigation bar with language options: English, العربية, Español, Français, Русский, and 中文. To the right of these options is a search bar labeled 'Search ICANN.org' and links for 'Log In' and 'Sign Up'. Below this is a white navigation bar with the ICANN logo on the left and menu items: GET STARTED, NEWS & MEDIA, POLICY, PUBLIC COMMENT, RESOURCES, COMMUNITY, and IANA STEWARDSHIP & ACCOUNTABILITY. The main content area has a blue background with a pattern of hexagons. A large blue box on the left contains the heading 'KSK Rollover' and a paragraph: 'Looking for more details on the upcoming root KSK rollover? ICANN has published a detailed document outlining what to expect during the rollover process and how to better prepare.' Below this text is a dark blue button labeled 'Read now'. To the right of this box is a graphic of several hexagons containing icons: a calendar, a padlock, a computer monitor, a document, a globe with a warning sign, and a key with a circular arrow. Below the main content area, there are two white boxes. The left one is titled 'News and Announcements' and contains a link: 'Moving Forward with Registration Data Access Protocol (RDAP)'. The right one is titled 'Quicklinks' and contains a link: 'Accountability Indicators'.



Технология и бизнес

И снова, в который раз: как устроена система DNS

Довольно часто при рассмотрении принципов функционирования DNS как бизнес-процесса смешивают в «одну посуду» несколько совершенно различных технологических процессов. А их как минимум три:

- управление реестром имен,
- делегирование прав управления доменами,
- поддержка DNS-инфраструктуры (резолвинг).



Реестр

Регистрация прав на управление доменом в реестре непосредственно к самой системе DNS как к технологическому процессу трансляции имени отношения не имеет. Регистраторы с реестром взаимодействуют по протоколу EPP. В рамках этого взаимодействия в базе данных реестра создается множество объектов, например:

- Domain – описывает доменное имя и параметры его регистрации;
- Host – описывает серверы доменных имен, которые поддерживают домены;
- Contact – описывает данные администратора домена;
- Registrar – описывает параметры регистратора.

¹ RFC-4786



Делегирование

Связь с процессом трансляции имени у реестра появляется тогда, когда реестр генерирует и выгружает на DNS-сервер файл зоны, где каждому домену поставлены в соответствие серверы доменных имен, которые обслуживают домены.

```
dig example.com
```

```
example.com.      821 IN  A    93.184.216.34
```

```
;; AUTHORITY SECTION:
```

```
example.com.      86306 IN  NS   b.iana-servers.net.
```

```
example.com.      86306 IN  NS   a.iana-servers.net.
```

```
;; ADDITIONAL SECTION:
```

```
b.iana-servers.net. 191 IN  A    199.43.133.53
```

```
b.iana-servers.net. 191 IN  AAAA 2001:500:8d::53
```

```
a.iana-servers.net. 191 IN  A    199.43.135.53
```

```
a.iana-servers.net. 191 IN  AAAA 2001:500:8f::53
```

Инфраструктура

- Протокол DNS, который реализован на серверах доменных имен и резолверах.
- Он помогает использовать систему DNS в качестве большой поисковой машины.
- При этом машины универсальной.
- Дерево доменов позволяет быстро, и это ключевое свойство системы, искать как IP-адреса по заданным именам, так и имена по заданным адресам.



В поиске альтернатив: DNS и Blockchain

«Есть ли практический способ разделить единственное имя между конкурирующими реестрами?»

J.Postel (1996)

Если не углубляться в криптографические подробности, то технология Blockchain позволяет вести распределенный реестр всего, чего угодно. И раз в системе DNS есть реестры, то было бы грех не попробовать реализовать их на этой новой технологии.

Итак, мы имеем как минимум двух претендентов на реализацию:

- реестр доменов верхнего уровня;
- реестр изменений файла зоны.



Как это сделано

NameCoin – это одно из первых ответвлений от Bitcoin (2010).

Мотивация создателей NameCoin проста – создать децентрализованную, защищенную от цензуры и вмешательства извне систему доменных имен, альтернативную существующей (навеяло SOPA).

Для реализации реестра и системы DNS не нужны DNSSEC и прочие ухищрения. Достоверность информации, в нашем случае — принадлежность имени администратору и соответствие имени конкретному адресу, обеспечивается самой технологией Blockchain.

Достоинства/недостатки:

- «Реестр» и «DNS» размещены у пользователя
- Поиск соответствия быстрее, чем традиционной DNS
- На любую операцию с доменом нужно ~ 2 часов
- Опыта ведения реестра имен в сотни миллионов штук нет

Как это сделано (2)

Еще одна альтернатива традиционной системе DNS на основе технологии Blockchain является система **ENS (Ethereum Name Service)**, построенная на основе smart-контрактов системы Ethereum.

Система технологически состоит из двух типов компонентов:

- Реестра;
- Резолвера.

Реестр содержит информацию для всех доменов и поддоменов об администраторе домена, резолвере домена и времени жизни всех ресурсных записей, которые связаны с доменом.

Главное назначение резолвера – обеспечивать поиск соответствия между именем и адресом. При этом в документации оговаривается, что поиск соответствия предполагает нечастое обновление этого самого соответствия.

Регистратор в системе ENS — это smart-контракт, который регистрирует домены в соответствии со спецификацией EIP 162 [11].

В случае, когда на регистрацию одного и того же имени претендует несколько клиентов, включается аукцион доменов. Длительность типового аукциона пять дней. Платят за регистрацию Эфиром (монета Ethereum).



Вопросы, которые «лежат на поверхности»

- Как изменятся бизнес-процесс? Например, что будет с обратными зонами?
- Как, кому и за что будут платиться деньги?
 - Майнерам?
 - Владельцам контрактов?
 - ...
- Как будет формироваться цена? Динамически? На конкурентной основе?
- Готов ли конечный пользователь платить за каждое изменение?
(Например, изменение IP-адреса)
- Что делать с динамическим DNS?
- Два часа на подтверждение изменений – это приемлемо?
- Как будет себя вести технология при обслуживании 332 миллионов доменных имен?



Вопросы?