Blockchain и DNS

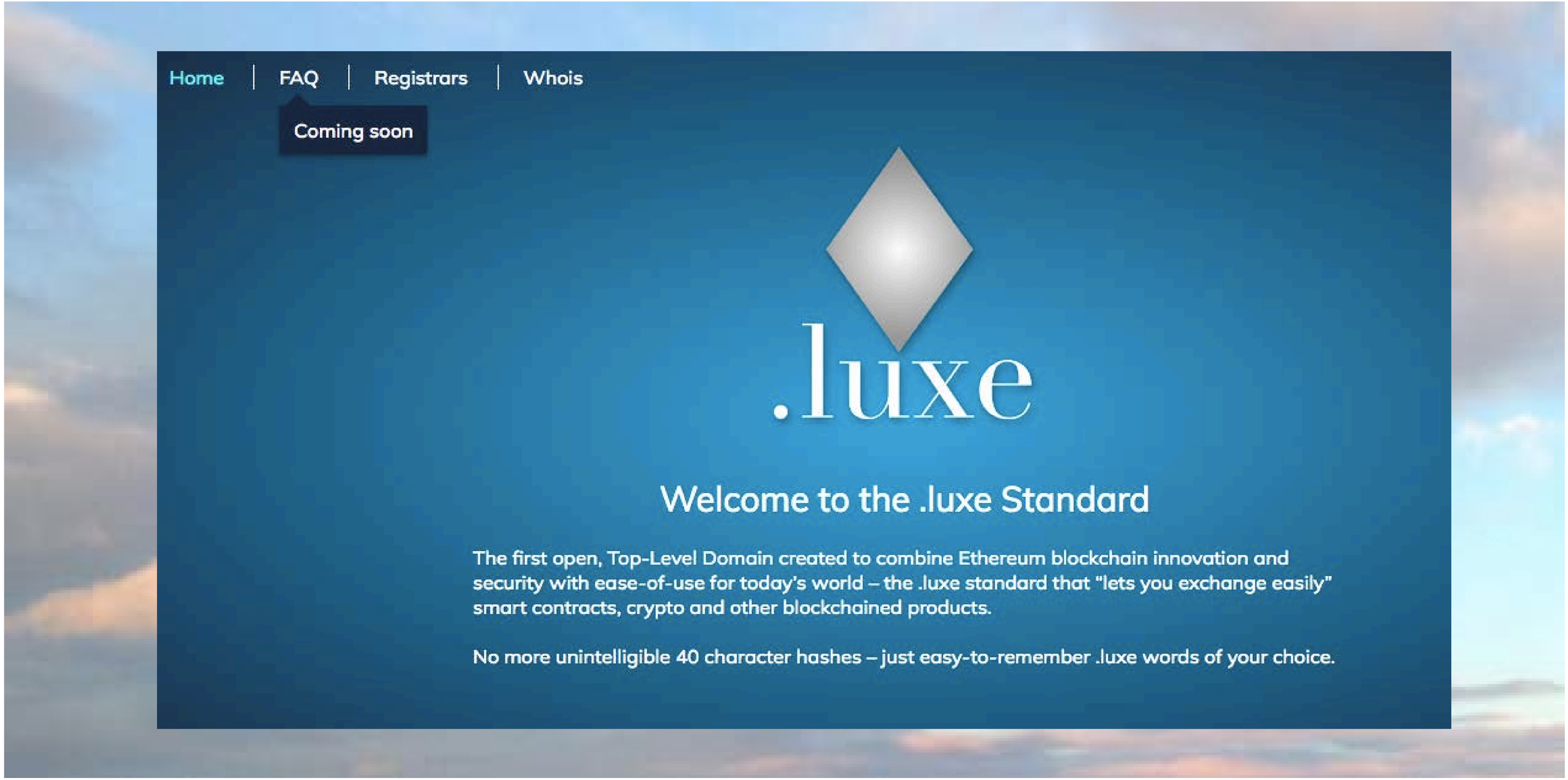
Воспоминание о будущем

Павел Храмцов
p.khramtsov@msk-ix.ru

TLDCON-2018
RIGA

Технический Центр Интернет

Не верь глазам своим

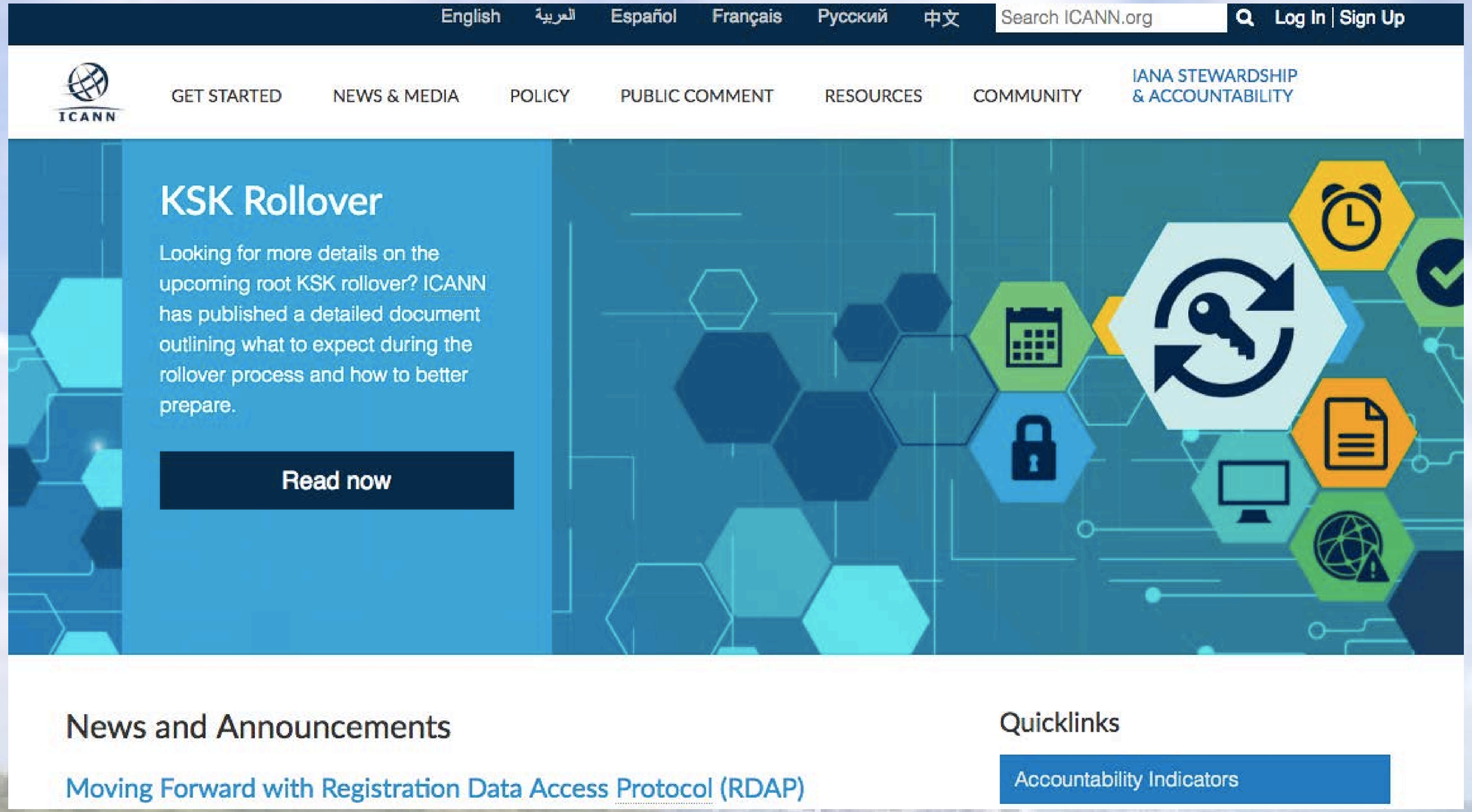


Павел Храмцов, MSK-IX, p.khramtsov@msk-ix.ru

MSK IX

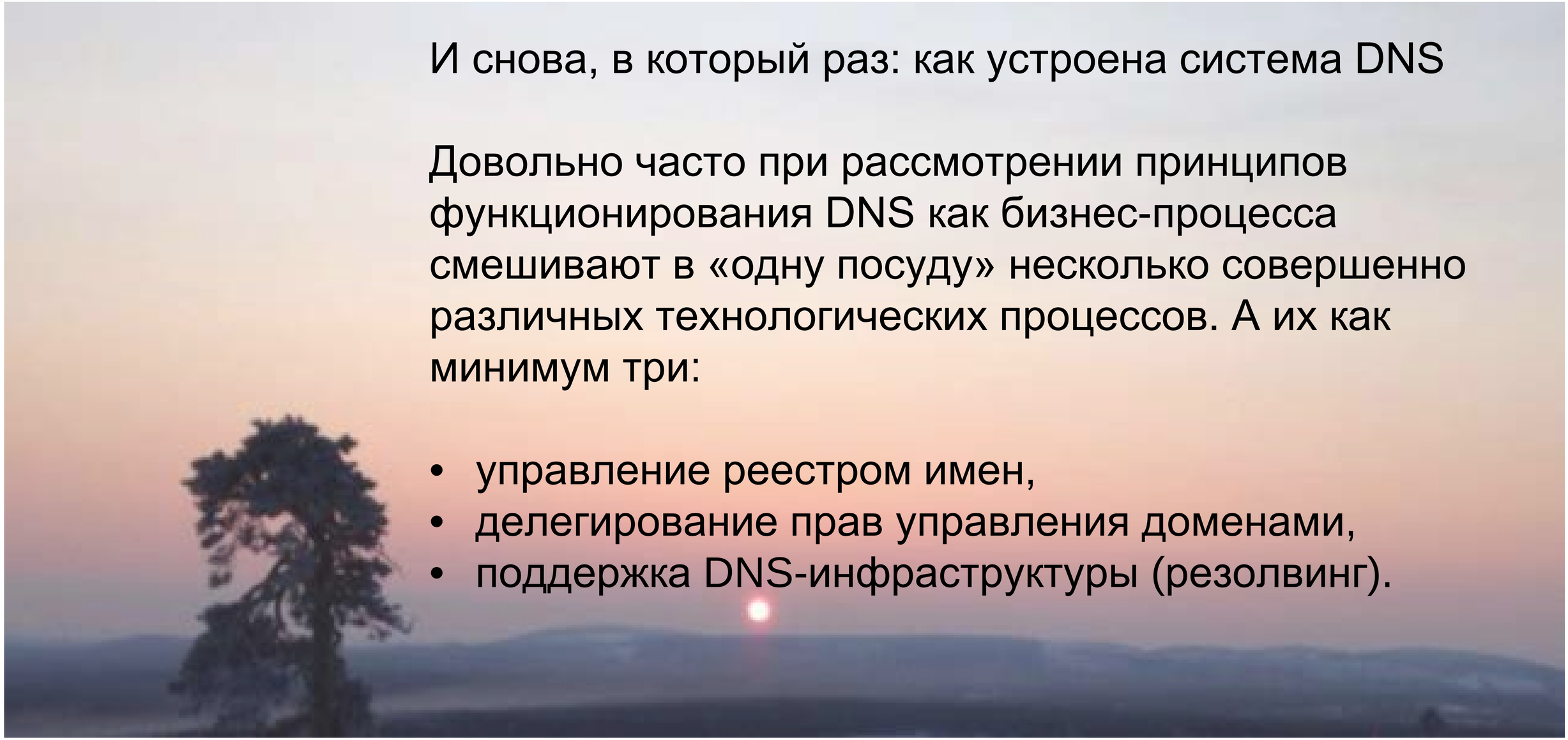
Технический Центр Интернет

20-летие ICANN



Технический Центр Интернет

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
```

Технический Центр Интернет

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 милионов 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?