Blockchain, IoT and DNS

ICANN64 Tech Day
Kobe, Japan
Tom Barrett
EnCirca President
About EnCirca

• Formed in 2001 in Boston, USA
• ICANN Accredited Registrar
• Specialty: Partnering with TLD Registries
  • Restricted and regulated TLDs
  • White-labelled Storefronts for DotBrand and regulated registries
  • Validation Provider for .BANK and six other TLDs
  • Blockchain integration with .LUXE, XYZ
Why Do We Care?

The blockchain and the Internet of Things (IoT) are two of the most transformative technologies in the world today.

“Blockchain technology is probably the best invention since the internet itself”
IoT Investments

Overall investments in IoT startups Q1 2017 – Q2 2018

- Q1 2017: 579 Investment ($M), 141 Deals
- Q2 2017: 730 Investment ($M), 153 Deals
- Q3 2017: 940 Investment ($M), 126 Deals
- Q4 2017: 646 Investment ($M), 92 Deals
- Q1 2018: 883 Investment ($M), 80 Deals
- Q2 2018: 874 Investment ($M), 113 Deals

Source: IoT Analytics Research, Postscapes
Blockchain Investments

[Bar chart showing capital invested and deal count from 2013 to 2018]
Blockchain and IoT

• Both need DNS to work.

• Both need features not present in today’s DNS

• Alternative frameworks and protocols are emerging to address the limitations of the DNS

• Will DNS advance to meet this challenge?

• What role will ICANN play in this space?
A World Exploding with Devices
IoT Defined

Connect physical things to communication networks with a special focus on:

• Existing infrastructure (buildings, roads, vehicles, factory equipment, etc.) and

• Constrained devices with extremely limited computing resources (switches, valves, sensors, actuators, thermostats, etc.)
Blockchain Defined

• An open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way

• A growing list of records, called blocks, are linked using cryptography

• Typically managed by a peer-to-peer network

• Data in any block cannot be altered retroactively without alteration of all subsequent blocks
Blockchain Benefits

• You have complete control of the value you own; there is no third party that holds your value or can limit your access to it.

• The cost to perform a value transaction from and to anywhere on the planet is very low. This allows micropayments.

• Anyone at any time can verify every transaction made on the blockchain, resulting in full transparency.

• It’s possible to leverage the blockchain technology to build decentralized applications that would be able to manage information and transfer value fast and securely.
Blockchain Application

WHAT IS THE CHAIN OF TITLE?

1. Grant deed from Jane Doe to John Doe dated 10/3/1927
2. Grant deed from John Doe to John Smith and Regina George dated 7/5/1949
Naming Infrastructure Needed

• IoT and Blockchain need Naming Infrastructures similar to DNS

• How Does DNS advance to support the Internet of Things?

• Are ICANN’s version of DNS and Blockchain compatible?
DNS is Relatively Old

• DNS was invented in 1983, 15 years before the birth of ICANN
• Security was not considered in the first RFC’s
• But DNS is continually evolving
  • DNSSEC to address security limitations
  • IPv6 to address IP address scarcity
  • IDN’s to support 80+ languages
IPv6 Makes IoT Possible

Total IPv6 addresses = $53 \times 10^{39}$ or 340 trillion, trillion trillion
IoT Challenges

• Scale
  • Estimated 25-50 billions devices by 2020

• Functionality
  • Constrained devices need zero or auto configuration

• Security
  • DNSSEC and ???

• Availability
  • From Millions to Billions of devices

• Performance (latency)
  • Humans tolerate latency
  • Autonomic applications can not tolerate latency
DNS Evolving for IoT

• Key DNS Standards
  • IPv6
  • DNSSEC
  • DNSNA – Name Autoconfiguration
  • ND – Neighbor Discovery
  • DNS Service Discovery (DNS-SD), which enables rapid discovery of local devices and services by making all devices multicast with each other in a peer-to-peer fashion
Will Traditional DNS scale for IoT?

• Missing confidentiality, integrity and encryption, Does not address DDOS attacks

• Fully distributed IoT devices require a decentralized basis for identity and discovery

• the DNS depends on a centralized trust model that it ultimately dependent on 13 root name servers, which is at odds with the decentralized ethos of open blockchains

• Enter technologies like Blockstack, Namecoin, and blockname

• These systems provide global, decentralized registries of "things" like device identities and keys, enabling more secure bootstrapping of communication and greater trust in the overall network
IoT Example: Geo-fencing
A **geo-fence** is a virtual perimeter for a real-world geographic area.

A geo-fence could be dynamically generated—as in a radius around a point location, or a geo-fence can be a predefined set of boundaries (such as school zones or neighborhood boundaries).
Image the room you’re in filled with sugar cubes

Each assigned a permanent, unique IPv6 address
IPv6 as a 3D Coordinate System
The IPv6 network and geolocation are now fused

Making places and IPv6 addresses interchangeable @ cm precision
Fence Delivery Network

• Leverages the DNS
• Global coordinate system maps each cubic centimeter (cm³) to IPv6 address
• Delivers SmartFences using DNSSEC
• Domain names are simple, memorable, meaningful

• .PLACE TLD will be exclusively used for Geo-Fencing

• Not a new idea! .GEO in 2000 round
Blockchain and Naming

Emerging Naming technologies that look like traditional DNS...without ICANN
Blockchain Naming

• Ethereum Blockchain
  • 41 million Ethereum identifiers
  • 99,000 new identifiers added every day in 2018
  • Crypto currency typically stored in Ethereum wallets
  • 35 million crypto wallets now in use

• Blockchain Wallet Example:
  
  0x25313a61bef2cd064a78c19acafcf5d951703a5f
35 Million Blockchain Wallets

Source: blockchain.com
Blockchain Domain Names

1. No central authority to decide which new TLDs are approved
2. Users control their domains and they can’t be taken away
3. Innovative Payments and Emerging ID Technology
Ethereum Naming Service

- ENS offers a secure & decentralized way to address resources both on and off the blockchain using simple, human-readable names.

- ENS features an automated registrar that allows anyone to register names ending in ".eth" using an auction process.

- Managing the ENS Root

- Root Key Holders exist for ENS
Payment Processing

“Digital Wallet”

EnCirca.eth

Payment routed to account

1CfaunqrVpcXmpLheUVWeSP1KPsKDha1Nb (Bitcoin)

0xbb9bc244d798123fde783fcc1c72d3bb8c189413 (Ethereum)

0718239283 (ABA routing number)

0xdjlkjMtyV5XQU26pzY6MGa5xYQR3blah (etc.)
Blockchain Naming

The Blockchain is solving the same problem for Digital Wallets that DNS solves for websites...

without the involvement of ICANN!
.ETH After 18 months

• 300,000 registrations

• $28 million in deposits

• Top domain sold for $3.5 million
## .ETH Compared to New gTLDs

<table>
<thead>
<tr>
<th>Rank</th>
<th>Domain</th>
<th>Registrations</th>
<th>Market Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>.icu</td>
<td>452,270</td>
<td>1.71%</td>
</tr>
<tr>
<td>12</td>
<td>.app</td>
<td>369,285</td>
<td>1.40%</td>
</tr>
<tr>
<td>13</td>
<td>.gdn</td>
<td>334,998</td>
<td>1.27%</td>
</tr>
<tr>
<td>14</td>
<td>.win</td>
<td>324,350</td>
<td>1.23%</td>
</tr>
<tr>
<td>15</td>
<td>.ooo</td>
<td>317,288</td>
<td>1.20%</td>
</tr>
<tr>
<td>16</td>
<td>.live</td>
<td>312,591</td>
<td>1.18%</td>
</tr>
<tr>
<td>17</td>
<td>.website</td>
<td>312,564</td>
<td>1.18%</td>
</tr>
<tr>
<td>18</td>
<td>.men</td>
<td>311,609</td>
<td>1.18%</td>
</tr>
<tr>
<td>19</td>
<td>.space</td>
<td>298,377</td>
<td>1.13%</td>
</tr>
<tr>
<td>20</td>
<td>.fun</td>
<td>250,329</td>
<td>0.95%</td>
</tr>
</tbody>
</table>

### .ETH In the Top 20
ICANN TLDs With Blockchain Integration

• .XYZ (Ethereum) – July 2018

• .LUXE (Ethereum) – August 2018

• .PID (Ethereum) – coming soon
Namecoin is an experimental open-source technology which improves decentralization, security, censorship resistance, privacy, and speed of certain components of the Internet infrastructure such as DNS and identities.

- *Bitcoin frees money*
- *Namecoin frees DNS, identities, and other technologies.*
Dot BIT

The “problem” with DNS is that DNS servers are controlled by governments and large corporations, and they could abuse their power to censor, hijack, or spy on your Internet usage. This happens on a regular basis across the world, including in countries like China as well as in countries like the United States.

Dot-Bit’s Solution

Dot-Bit-enabled websites address this issue because instead of the DNS controlled by a corporation or government, the DNS resides on your own computer. Bitcoin technology ensures that every user in the world has the same DNS data on their computer, without anyone being able to “illegitimately” change that DNS data.
A Crowdsourced DNS of Things

**Moeco** is built to become a DNS of things — a platform integrating various connectivity standards and connecting billions of devices across the globe.

**Moeco** uses crowdsourcing to gain coverage and help businesses effortlessly adopt IoT technology in a most cost-effective way.
Blockchain-only TLDs

- .BIT – (Bitcoin) - 2013
- .ETH – (Ethereum) – 2017
- .ZIL (Zilliqa) – 2019
- .CRYPTO (Ethereum) - 2019
- And many more!

- All require a special browser/plug-in
- We’ve seen this before...New.Net (circa 2003-10)
OpenNIC Sales Pitch

• *Looking for an open and democratic alternative DNS root? Concerned about censorship?*
  • DNS Neutrality (No censorship or IP rights)
  • No Cost
  • Stop DNS Hijacking (from ISP’s)

• Accessible Alternative TLDs via Browser Plug-ins

<table>
<thead>
<tr>
<th>.bbs</th>
<th>.chan</th>
<th>.cib</th>
<th>.dyn</th>
<th>.geek</th>
</tr>
</thead>
<tbody>
<tr>
<td>.gopher</td>
<td>.indy</td>
<td>.libre</td>
<td>.neo</td>
<td>.null</td>
</tr>
<tr>
<td>.o</td>
<td>.oss</td>
<td>.oz</td>
<td>.parody</td>
<td>.pirate</td>
</tr>
<tr>
<td>.bit</td>
<td>.lib</td>
<td>.coin</td>
<td>.bazar</td>
<td>.fur</td>
</tr>
</tbody>
</table>
“Benefits” Over ICANN TLDs

• Security
• Privacy
• Censorship-Resistance
• Scalability
• Faster
• Free and Open Source Software
• DNS Anonymity Networks (Tor, P2P)
Could Blockchain Replace DNS?

• Unlike the current DNS system which is governed and is controlled by organizations, Blockchain-based DNS does not have any authorities.

• Every node in the server is equal (no hierarchy).

• Only the owners can make changes in the current records. It is difficult for the authorities to make any changes in the domain name records (i.e. censorship).

• The current DNS system is prone to attack and hacking, but this is not the case with Blockchain-based DNS (in theory).
ICANN Mission vis-à-vis Blockchain TLDs

*ICANN’s mission is to help ensure a stable, secure and unified global Internet.*
Thank You

Thomas Barrett
EnCirca President

tbarrett@encirca.com
https://www.linkedin.com/in/thomasbarrett/