

# Blockchain, IoT and DNS

ICANN64 Tech Day  
Kobe, Japan  
Tom Barrett  
EnCirca President

# About EnCirca

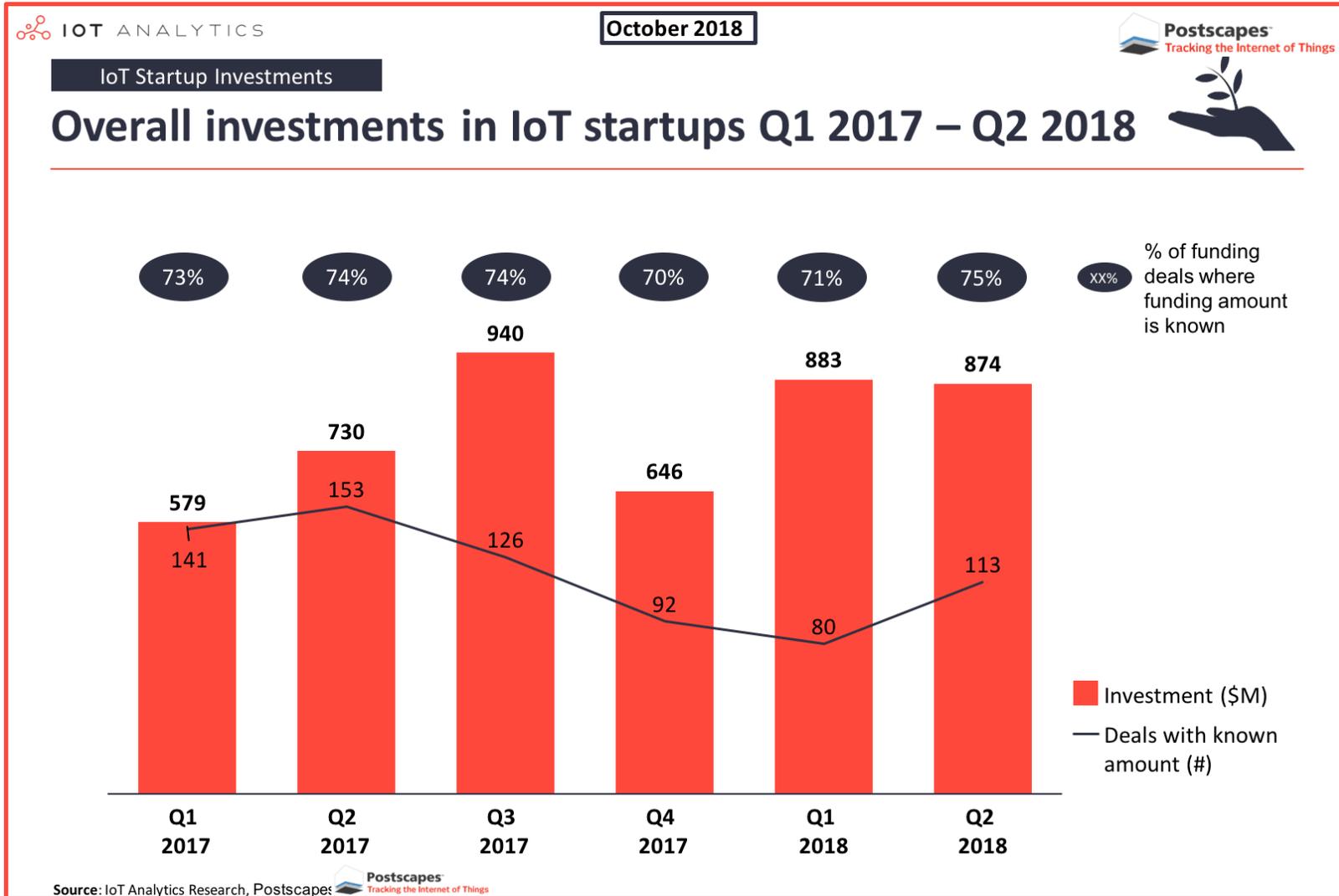
- Formed in 2001 in Boston, USA
- ICANN Accredited Registrar
- Specialty: Partnering with TLD Registries
  - Restricted and regulated TLDs
  - White-labelled Storefronts for DotBrand and regulated registries
  - Validation Provider for .BANK and six other TLDs
  - Blockchain integration with .LUXE, XYZ

# Why Do We Care?

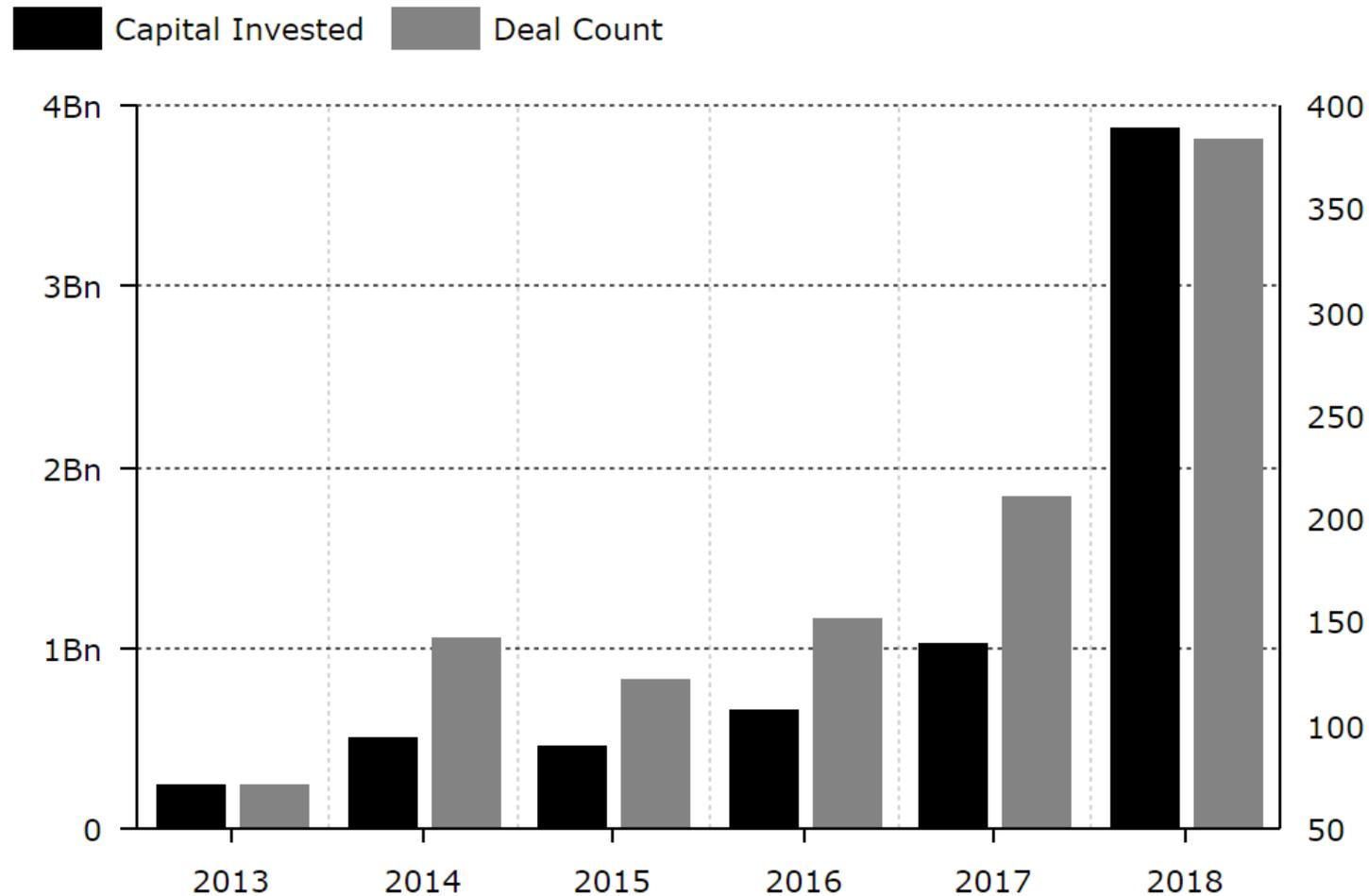
The blockchain and the Internet of Things (IoT) are two of the most transformative technologies in the world today.

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

# IoT Investments (millions)



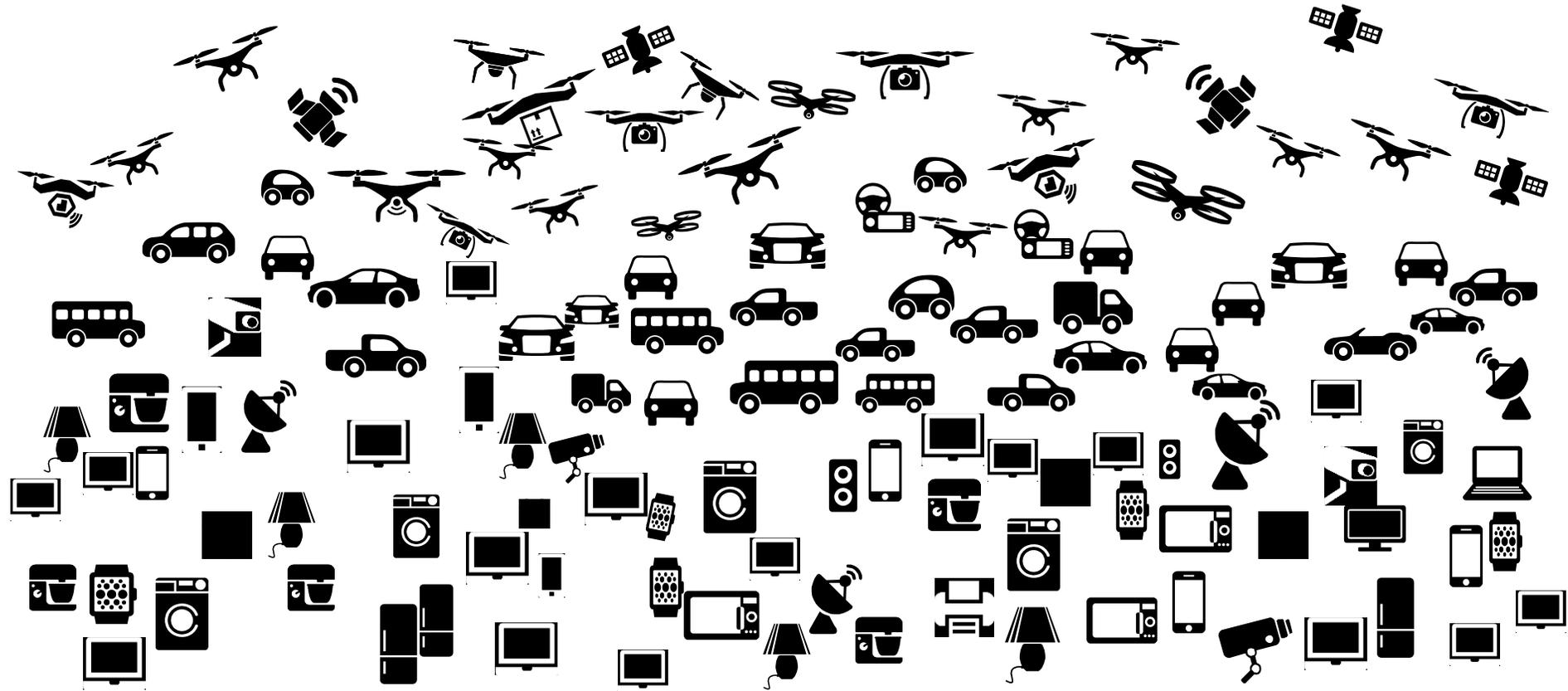
# Blockchain Investments (billions)



# 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 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

3. Warranty Deed from John Smith and Regina George to Harvey Dent and Gretchen Wieners dated 3/24/1970.

4. Deed to Secure Debt from Harvey Dent and Gretchen Wieners to the Gotham Metropolis Bank dated 5/16/1977.

# 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 compatible with Blockchain?

# 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

IPv4 →

IPv6 →

$2^x$	$10^x$	Decimal	IP Quantity	Short Scale	SI Prefix	Equivalent Quantities
$2^8$	$\approx 10^2$	256	Single IPv4 interface (/24)			
$\approx 2^{10}$	$10^3$	1,000			kilo	
$2^{16}$	$\approx 10^5$	65,536	IPv4 Class B (/16)			
$\approx 2^{17}$	$10^5$	100,000				
$\approx 2^{20}$	$10^6$	1,000,000		million	mega	
$2^{24}$	$\approx 10^7$	16,777,216	IPv4 Class A (/8)			
$\approx 2^{30}$	$10^9$	1,000,000,000		billion	giga	Base pairs in the human genome ( $3 \times 10^9$ ).
$2^{32}$	$\approx 10^9$	4,294,967,296	Entire IPv4 space			
$\approx 2^{40}$	$10^{12}$	1,000,000,000,000		trillion	tera	Bacteria on you.
$\approx 2^{50}$	$10^{15}$	1,000,000,000,000,000		quadrillion	peta	Ants on earth.
$\approx 2^{60}$	$10^{18}$	1,000,000,000,000,000,000		quintillion	exa	Meters light travels in 100 years.
$2^{64}$	$\approx 10^{19}$	18,446,744,073,709,551,616	Single IPv6 interface (/64)			
$\approx 2^{70}$	$10^{21}$	1,000,000,000,000,000,000,000		sextillion	zetta	Grains of sand on earth's beaches.
$\approx 2^{80}$	$10^{24}$	1,000,000,000,000,000,000,000,000		septillion	yotta	Stars in the universe.
$2^{80}$	$\approx 10^{24}$	1,208,925,819,614,629,174,706,176	IPv6 Site (/48)			
$\approx 2^{90}$	$10^{27}$	1,000,000,000,000,000,000,000,000,000		octillion		Atoms in you ( $7 \times 10^{27}$ ).
$2^{96}$	$\approx 10^{29}$	79,228,162,514,264,337,593,543,950,336	IPv6 ISP/Large enterprise (/32)			
$\approx 2^{100}$	$10^{30}$	1,000,000,000,000,000,000,000,000,000,000		nonillion		Bacterial cells on earth ( $5 \times 10^{30}$ ).
$\approx 2^{110}$	$10^{33}$	1,000,000,000,000,000,000,000,000,000,000,000		decillion		Mass of the Sun in grams ( $2 \times 10^{33}$ ).
$2^{116}$	$\approx 10^{35}$	83,076,749,736,557,242,056,487,941,267,521,536	IPv6, RIR (/12)			
$\approx 2^{120}$	$10^{36}$	1,000,000,000,000,000,000,000,000,000,000,000,000		undecillion		Ratio of force of electromagnetism to gravity.
$2^{125}$	$\approx 10^{37}$	42,535,295,865,117,307,932,921,825,928,971,026,432	IPv6 GUA (2000::/3)			
$2^{128}$	$\approx 10^{38}$	340,282,366,920,938,463,463,374,607,431,768,211,456	Entire IPv6 space			
$\approx 2^{130}$	$10^{39}$	1,000,000,000,000,000,000,000,000,000,000,000,000,000,000		duodecillion		Molecules of H <sub>2</sub> O in Great Lakes ( $53 \times 10^{39}$ ).

Recall that the character  $\approx$  means *approximately equal to*.

Total IPv6 addresses =  $3.4 \times 10^{38}$  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
  - Autonymous 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)

Imagine the room you're in  
filled with sugar cubes

Each assigned a permanent,  
unique IPv6 address

# IPv6 as a 3D Coordinate System

**EnCirca**  
SOC 2 CERTIFIED  
Domain Name Registrar



# Fence Delivery Network

- Leverages the DNS
- Global coordinate system maps each cubic centimeter (cm<sup>3</sup>) 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

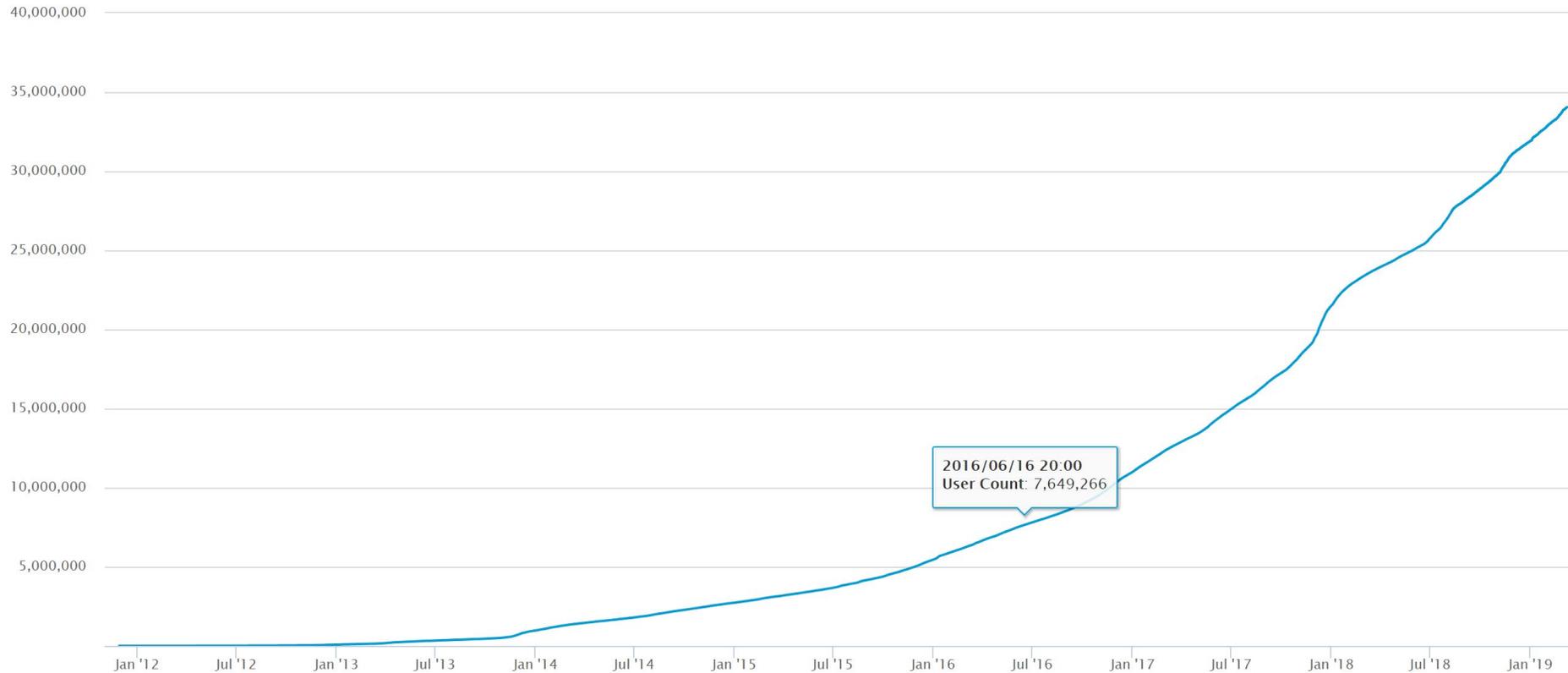


# Blockchain and Naming

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

# Blockchain Exploding

Source: blockchain.com



# Blockchain Wallets

Blockchain Wallet Example:

0x25313a61bef2cd064a78c19acafcf5d951703a5f

If only...

there was a more-friendly way  
to name my wallet?

# 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

# The .ETH Top-Level-Domain

(After 18 months)

- A Blockchain-only TLD (BTLDs)
- 300,000 registrations
- \$28 million in deposits
- Top domain sold for \$3.5 million

# .ETH Compared to New gTLDs

11	<a href="#">.icu</a>	452,270	1.71%			
12	<a href="#">.app</a>	369,285	1.40%			
13	<a href="#">.gdn</a>	334,998	1.27%			
14	<a href="#">.win</a>	324,350	1.23%			
15	<a href="#">.ooo</a>	317,288	1.20%			
16	<a href="#">.live</a>	312,591	1.18%			
17	<a href="#">.website</a>	312,564	1.18%			
18	<a href="#">.men</a>	311,609	1.18%			
19	<a href="#">.space</a>	298,377	1.13%			
20	<a href="#">.fun</a>	250,329	0.95%			

**.ETH In the Top 20**

# Blockchain Wallets

Blockchain Wallet “Domain”:

EnCirca.eth →

0x25313a61bef2cd064a78c19acafcf5d951703a5f

Branded Blockchain TLDs Possible too!

Tom.EnCirca →

0x25313a61bef2cd064a78c19acafcf5d951703a5f

# Blockchain Naming

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

without the involvement of ICANN!

# 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



# Blockchain TLDs (BTLDs)

<b>.bit</b> <b>(2013)</b>	<b>.eth</b> <b>(2017)</b>	<b>.zil</b> <b>(2019)</b>	<b>.crypto</b> <b>(2019)</b>	
.bbs	.chan	.cib	.dyn	.geek
.gopher	.indy	.libre	.neo	.null
.o	.oss	.oz	.parody	.pirate
.bit	.lib	.coin	.bazar	.fur

# BTLD “Benefits” Over GTLDs

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

# Blockchain TLD vs ICANN TLD

- 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)

# Plug-in Required

- All BTLDs require a special browser/plug-in
  - We've seen this before...New.Net (circa 2003-10)
- Work-around: Integrate with a TLD already in ICANN's root
  - .XYZ (Ethereum) – July 2018
  - .LUXE (Ethereum) – August 2018
  - .PID (Ethereum) – coming soon

# What if?

What would happen if a dominant market force like fill-in-the-blank were to enter the cryptocurrency market on a massive scale and begin accepting cryptocurrencies as a payment method?

- Wechat
- J. P. Morgan
- Facebook
- Alibaba
- Amazon

# What if?

What would happen if a dominant market force like fill-in-the-blank were to enter the cryptocurrency market on a massive scale and begin accepting cryptocurrencies as a payment method?

Naturally, they might want to brand their blockchain wallets for customers....

Tom.Wechat  
Tom.JPMorgan  
Tom.Facebook  
Tom.Alibaba  
Tom.Amazon

# ICANN Mission vis-à-vis Blockchain TLDs

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

**Let's continue the conversation!**

**Thomas Barrett**  
**EnCirca President**

**[tbarrett@encirca.com](mailto:tbarrett@encirca.com)**

**<https://www.linkedin.com/in/thomasbarrett/>**