EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

Blockchain, IoT and DNS

ICANN64 Tech Day

Kobe, Japan

Tom Barrett

EnCirca President

About EnCirca

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

- 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

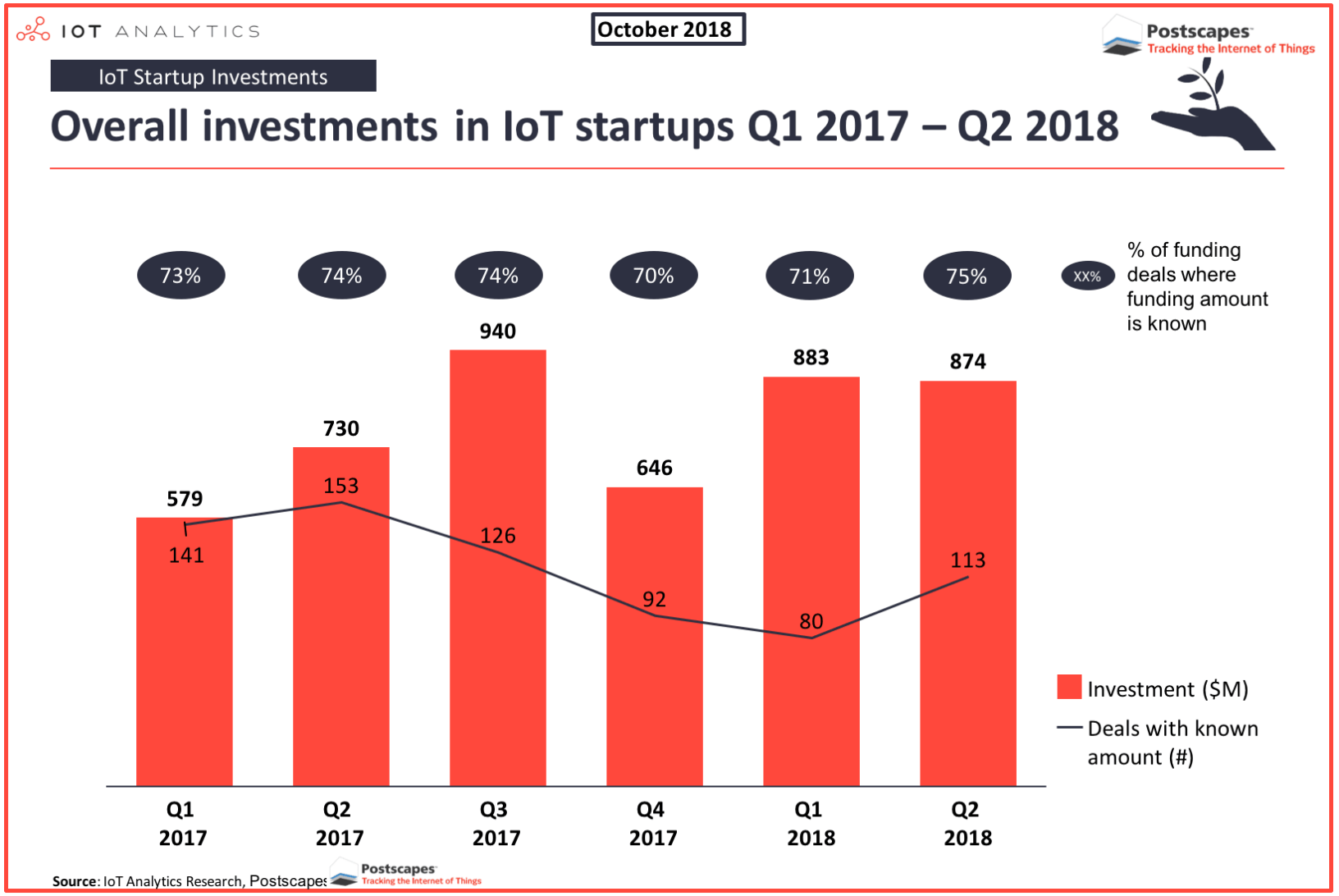
Why Do We Care?

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

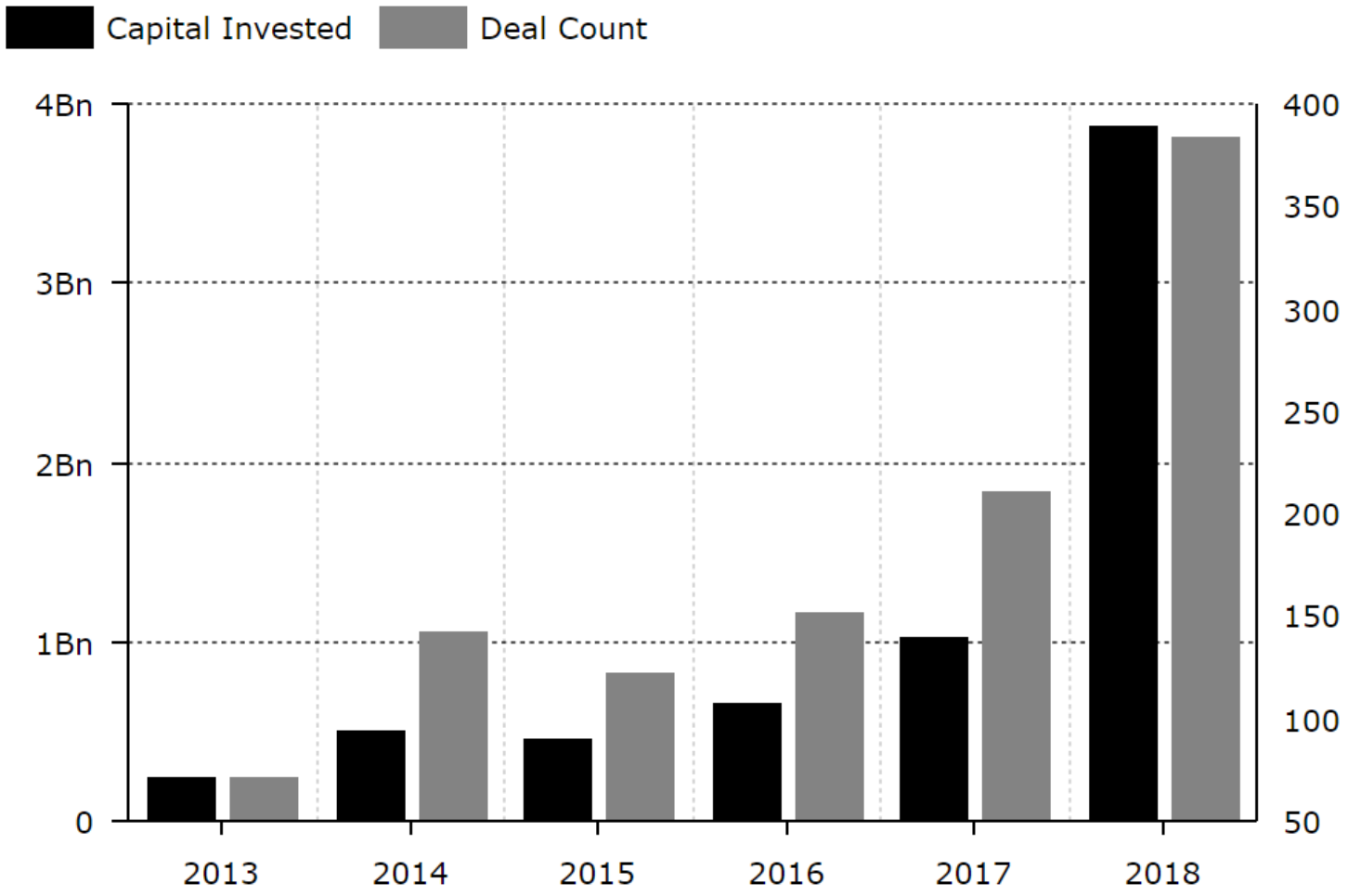
The blockchain and the Internet of Things (IoT) are two of the most transformative technologies in the world today.

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

IoT Investments



Blockchain Investments



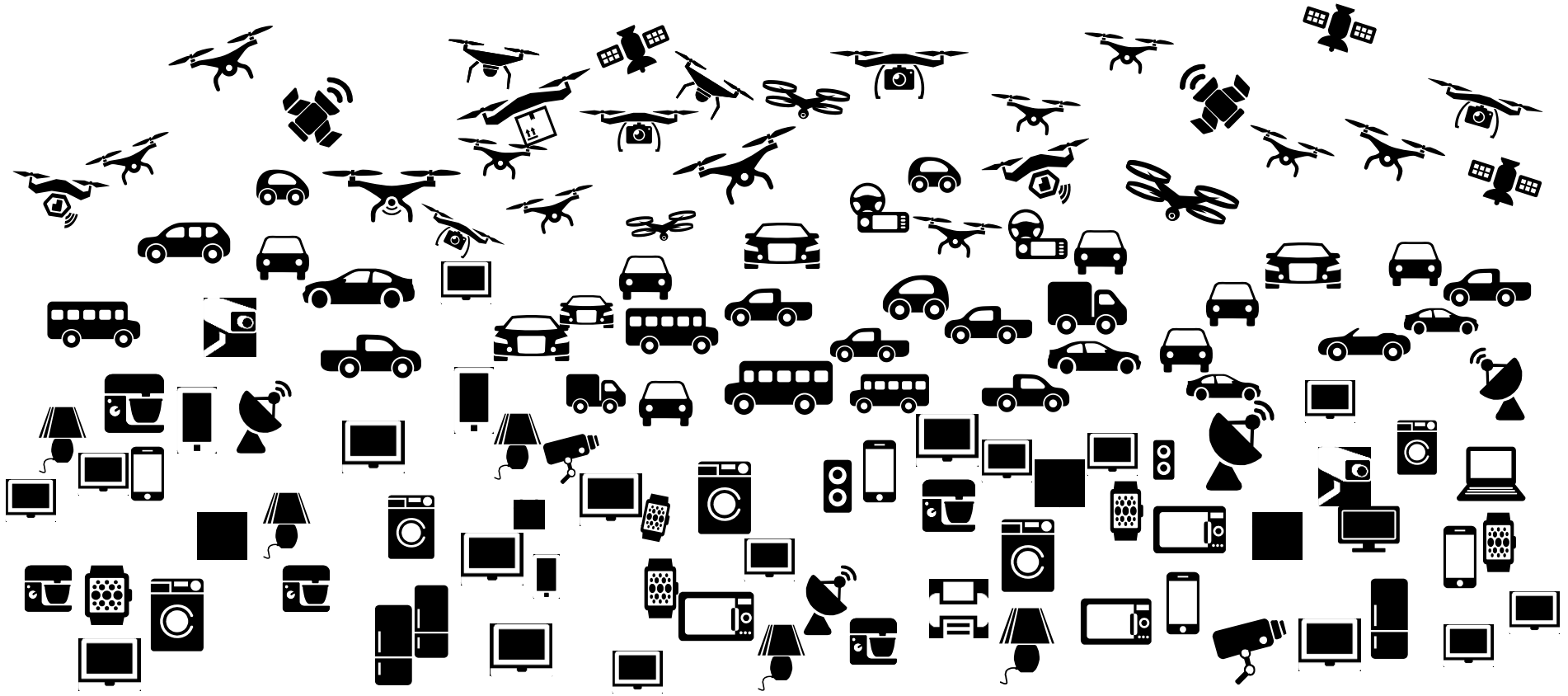
EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

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?

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

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

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

- 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

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

- 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

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

Naming Infrastructure Needed

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

- 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

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

- 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

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

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 ($3x10^9$).
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 ($7x10^{27}$).
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 ($5x10^{30}$).
$\approx 2^{110}$	10^{33}	1,000,000,000,000,000,000,000,000,000,000,000		decillion		Mass of the Sun in grams ($2x10^{33}$).
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		duodecillion		Molecules of H_2O in Great Lakes ($53x10^{39}$).

Recall that the character ≈ means *approximately equal to.*

Total IPv6 addresses = 53 x 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
    - Autonymous applications can not tolerate latency

DNS Evolving for IoT

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

- 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?

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

- 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

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

IoT Example: Geo-fencing

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)

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

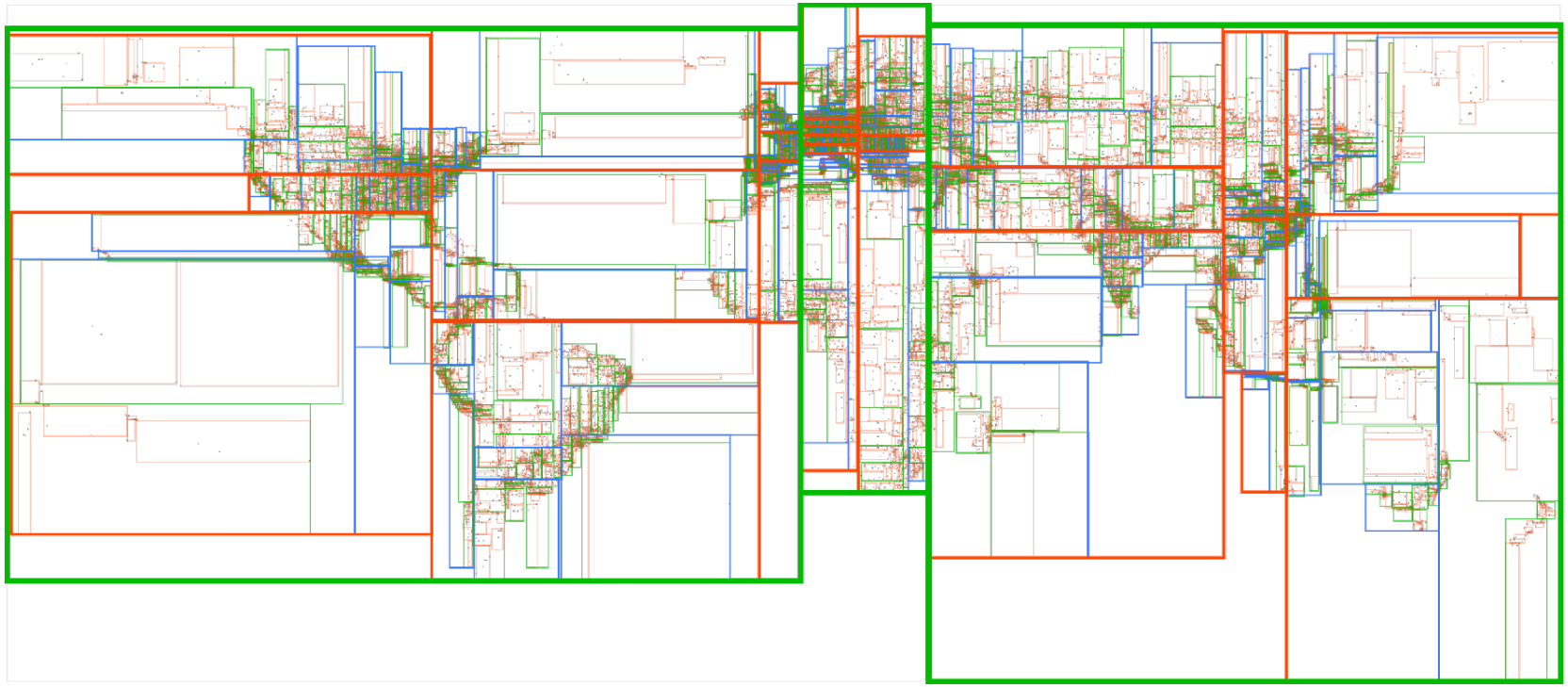
Image the room you're in filled with sugar cubes

Each assigned a permanent, unique IPv6 address

IPv6 as a 3D Coordinate System

The IPv6 network and geolocation are now fused

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar



Making places and IPv6 addresses interchangeable @ cm precision

Fence Delivery Network

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

- Leverages the DNS
- Global coordinate system maps each cubic centimeter (cm^3) 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

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

Blockchain and Naming

Emerging Naming technologies that look like traditional DNS…without ICANN

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

Blockchain Naming

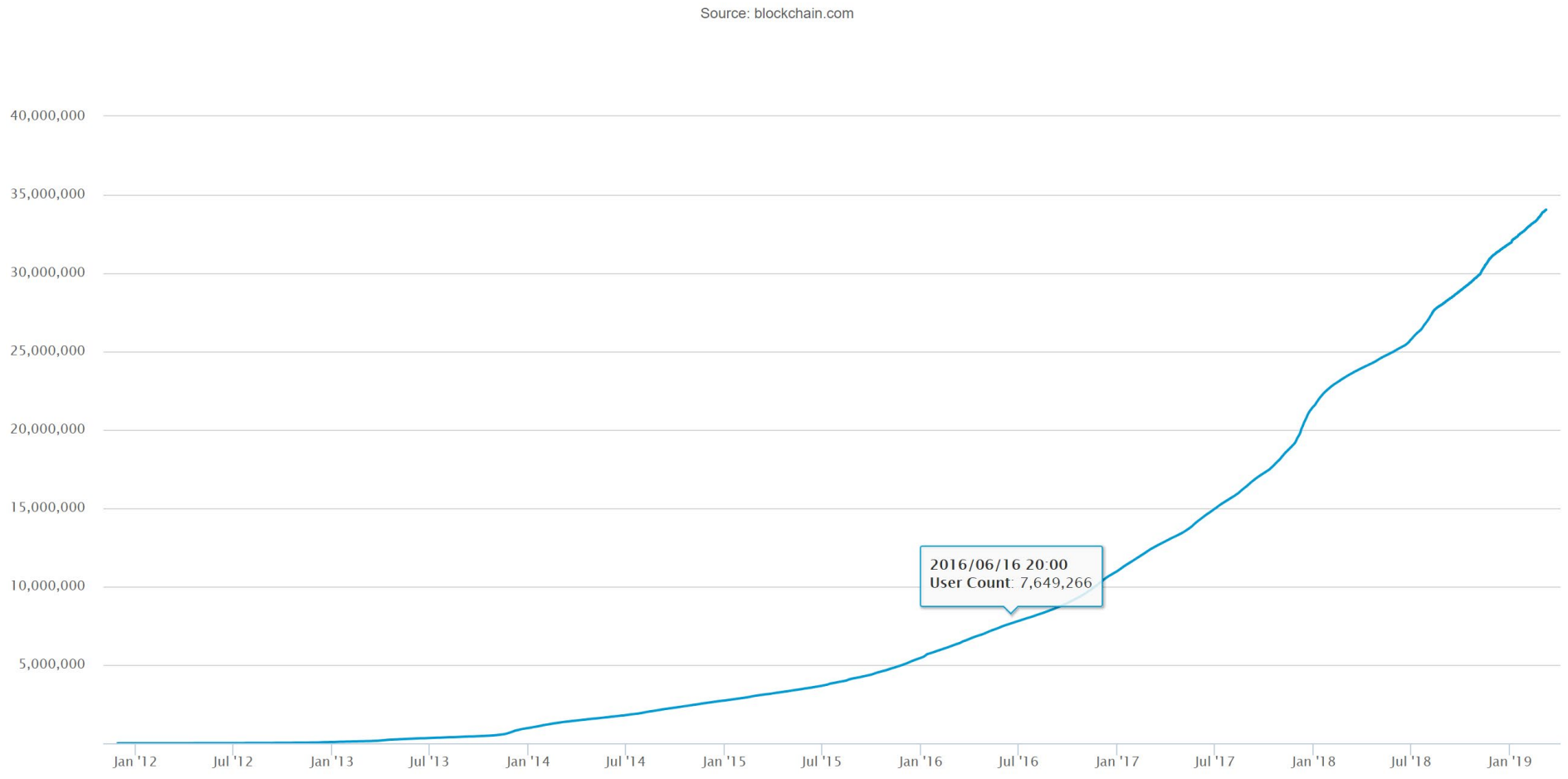
- Ethereum Blockchain
  - 41 million Ethereum identifiers
  - 99,000 new identifiers added every day in 2018
  - Crypto currency typically stored in Ethereum wallets
  - 35 million crypto wallets now in use

- Blockchain Wallet Example:

0x25313a61bef2cd064a78c19acafcf5d951703a5f

35 Million Blockchain Wallets

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar



Blockchain Domain Names

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

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

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

- 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

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

“Digital Wallet”

EnCirca.eth

Payment routed to account

1CfaunqrVpcXmpLheUVWeSP1KPsKDha1Nb (Bitcoin)

0xbb9bc244d798123fde783fcc1c72d3bb8c189413 (Ethereum)

0718239283 (ABA routing number)

0xjdjlkjMtyV5XQU26pzY6MGe5aXyQr3blah (etc.)

Blockchain Naming

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

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

without the involvement of ICANN!

.ETH After 18 months

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

- 300,000 registrations
- $28 million in deposits
- Top domain sold for $3.5 million

.ETH Compared to New gTLDs

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

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

.ETH In the Top 20

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

ICANN TLDs With Blockchain Integration

- .XYZ (Ethereum) – July 2018
- .LUXE (Ethereum) – August 2018
- .PID (Ethereum) – coming soon

Decentralized DNS

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

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

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

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

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

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

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

- .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

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

- *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

.bbs	.chan	.cib	.dyn	.geek
.gopher	.indy	.libre	.neo	.null
.o	.oss	.oz	.parody	.pirate
.bit	.lib	.coin	.bazar	.fur

“Benefits” Over ICANN TLDs

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

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

Could Blockchain Replace DNS?

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

- 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)

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

ICANN Mission vis-à-vis Blockchain TLDs

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

EnCirca
SOC 2 CERTIFIED
Domain Name Registrar

Thank You

Thomas Barrett
EnCirca President

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