ICANN & Distributed Ledger Technology (aka Blockchain): Evolution or Revolution?

By Michael Palage

NOTE: This is a preliminary draft which will be circulated for peer review over the next several weeks within the ISOC Blockchain Study Group and other invited individuals/entities. It is not intended for broader public circulation without permission of the author. A publication of final document is estimated to occur no later than the end of November 2017.

Executive Summary

Distributed Ledger Technology (DLT)/blockchain, the underlying technology powering Bitcoin, is quickly emerging as a transformative technology that is impacting a broad range of processes that have formed the foundation of e-commerce and social interaction over the past several decades.[1] One potential eco-system that will be impacted by this technology is the global domain name system administered by the Internet Corporation for Assigned Names and Numbers (ICANN), which currently serves as the global trustee/coordinator of this resource.

This paper will analyze some of the current distributed ledger technology proposals seeking to either enhance or potentially replace the domain name system (DNS). The DNS is simple layperson terms is like a telephone directory that maps a domain name (e.g. ISOC.ORG) to an IP Address (212.110.167.157). Given that the existing DNS resolves over 100 billion resolutions per day, it is critically important that ICANN and the broader Internet community engage in a constructive dialog with this community to find a constructive path forward.

ICANN 101 Overview

ICANN serves as the global coordinator of the Internet's unique identifiers (domain names and IP addresses). These functions include but are not limited to: preserving the security and stability of the Internet (e.g. SSAC); fostering the multi-stakeholder bottom up consensus driven policy model; contractual compliance of ICANN sanctioned gTLD registration authorities (registries and registrars); and the operation of key Internet Infrastructure (L Root and .INT Registry). These herculean tasks are not inexpensive with ICANN having an annual operational budget of over 130 million dollars, with upwards of an additional 300 million dollars held in various strategic reserves.

Despite this diverse portfolio of responsibilities, ICANN is disproportionately reliant on generic top-level domain names to fund over 97% of its operations. Given this single point of failure in its business model, ICANN has recently begun to evaluate potential technologies that might diminish or replace the domain name system. In 2013, Paul Mockapetris, the inventor of the DNS, chaired a blue-ribbon panel of experts to analyze emerging Identifier Technology Innovation as part of former ICANN CEO Fadi Chehadé's Strategy Panel initiative.

---

[1] For the purposes of this paper, the terms DLT and blockchain will be used interchangeably. However, it is important to understand that blockchain (both permissioned and permissionless) are a species within the broader DLT genus.

Blockchain Overview

Blockchain is a peer-to-peer DLT that provides for the secure archival of information (transactions) in a dynamic repository comprised of a never-ending series of sequential data blocks chained together using public/private key cryptography. Through the use of cryptography and consensus protocols associated with the writing of data blocks to the chain, the information stored in the repository is tamper resistant and immutable. It is this combination of features which provides the level of transparency, trust and accountability among users of that blockchain.

There are two general classifications of blockchain technology: permissioned and permissionless. The original Bitcoin blockchain was built to create a 'permissionless' peer-to-peer network for transferring a virtual currency from any one party on the network to any other party on the network. It is permissionless because there is no trusted authority (such as a bank or clearing house) verifying that the transactions are legitimate and that the record for the transactions is, and remains, correct. Instead, transactions are verified by a proof of work consensus protocol.

The proposed DLT/blockchain technologies discussed in this paper seeking to improve upon the existing DNS do so in their quest to solve all three legs of Zooko's Triangle. Zooko Wilcox-O'Hearn, an American computer security specialist, identified three desirable qualities in any network protocol: human meaningful; secure; and decentralized. He posited that it was only possible to achieve two of these three qualities. However, DLT/blockchain technology potentially opens the door to achieving all three of these qualities simultaneously. While the current DNS potentially satisfies two of these qualities (human meaningful and security), there exist several centralized chokepoints in the governance layer that prevents the Zooko's triangle trifecta. It is this drive toward a peer to peer naming system with enhanced privacy protection and immune from potential censorship that is driving much of this technology.

Namecoin

Namecoin was one of the first initiatives to explore the use of DLT/blockchain technology to potential replicate the functionality of the DNS. In fact, Namecoin was specifically referenced in ICANN's final May 2014 Identifier Technology Innovation Report, stating "[t]his might seem like a fantasy, but Byzantine algorithms like Bitcoin [Andreesen 2014] and Namecoin show that such systems are possible today." In March 20017, Jeremy Rand, lead application engineer at Namecoin, participated in ICANN's inaugural Emerging Identifiers Technology public panel at ICANN 58 in Copenhagen.[2]

The Namecoin software can serve three distinction functions: naming and resolution; digital identity; and cryptocurrency. Although the Namecoin does not promote itself as a commercial facing cryptocurrency, it is a publicly traded crypto currency (NMC). Namecoin at a core technical level in its own words is a "key/value pair registration and transfer system based on the Bitcoin technology." In layperson terms a user registers a name and stores associated values to it on the blockchain. Software then can access the blockchain to retrieve the stored values to resolve a name request.

The cost associated with registering a domain name is 0.01 NMC (include current $ price point), which includes both a registration fee and a transactions fee. The registration fee is currently voided (no gets it) and the transaction fee is determined by the miner, like the BitCoin business model. Unlike

[2] See https://www.namecoin.org/files/videos/icann-58/Namecoin-ICANN58-EIT-Final.pdf

traditional domain names which are register for a fixed period (i.e. yearly increments), Namecoin names are registered for a fixed number of blocks (35,999), which currently spans between 200 and 250, before a name needs to be renewed or updated.

Namecoin currently operates the non-ICANN sanctioned .BIT top level domain, although it is seeking to have it designated a Special Use Name (e.g. .ONION). The Namecoin software has incorporated a DNS compatibility layer to translate DNS requests into Namecoin requests, however, this software needs to be configured on each use's machine. Namecoin readily acknowledges that its software is an "experiment" and that there remain several unresolved shortcoming including, but not limited to: the inability to undo an accidental or fraudulent name transfer without the assistance of the current name holder; minimal trademark owner safeguards; lack of privacy (all transactions are public), etc.

Ethereum Naming System (ENS)

Unlike other DLT/blockchain technologies, ENS was initially conceptualized as a way to map human-readable names to hexadecimal Ethereum wallet and smart contract addresses, but its functionality can be extended to include other kinds of resources such as DNS records. Built as a protocol layer on top of the Ethereum blockchain, ENS provides a distributed lookup service for any kind of record, and is secured by one of the most robust blockchains in the world.

The ENS soft launch in May 2017 saw 180,822 names being registered, over an eight-week period. Approximately ETH168,595 (~US$50m) was committed by users in the auction-based distribution process, and the deposits will be locked up for a minimum period of one year, after which users will be able to retrieve their deposits if they relinquish those names.

Over the past few months, Ethereum Foundation has engaged in active discussions about name management, governance, DNS integration, and architectural design for ENS, reaching out to multiple stakeholders such as registries, registrars, crypto-wallet providers, and cryptocurrency exchanges. ENS also participated in a recent panel discussion on DLT/blockchain technologies at ICANN's regional meeting Abu Dhabi. ENS is in active dialog with one or more TLDs to integrate DNS names into ENS, and they have already implemented a prototype on the Ethereum testnet as a proof-of-concept.

As an organization, ENS is approaching the problem of governance more cautiously than other groups that have proposed new distributed identifier systems, and has built in safeguards in order to handle such issues. In their own words:

> To facilitate the possibility of upgrades and maintenance, and in exceptional circumstances to handle problems with ENS, the ENS root will initially be owned by a multisig, with members of the Ethereum dev community as keyholders. In the long term, we would like to see the root multisig replaced by some form of distributed decision making process, but developing such a process will require time, thought, and care, which we anticipate will be a longer term effort than the development of the permanent .eth registrar.

This proactive approach has permitted ENS to identify that the proposed .ETH string will likely give rise to potential geo-political concerns based on that string corresponding to the ISO-3166 List 3 designation for Ethiopia. This continued engagement will permit ENS to leverage lessons learned from ICANN's own governance growing pains.

Blockstack

Blockstack is probably the most revolutionary of the DLT/blockchain technologies currently available. Their rather audacious goals are front in center in its original whitepaper where in the first three sentences its states in clear and unequivocal terms that:

> The traditional internet has many central points of failure and trust, like (a) the Domain Name System (DNS) servers, (b) public-key infrastructure, and (c) end-user data stored on centralized data stores. We present the design and implementation of a new internet, called Blockstack, where users don't need to trust remote servers. We remove any trust points from the middle of the network and use blockchains to secure critical data bindings.

The vision of Blockstack is to create a paradigm shift where developers build applications using their protocol to empower users to retain control over their own data(identity) across one or more online storage repositories instead of the current paradigm where that user data is centralized by service providers where it can be viewed, altered, and/or monetized without the user's consent or knowledge. To achieve this objective, Blockstack is built upon three founding design goals: dencentralized naming and discovery; decentralized storage; and comparable performance to existing internet resources.

The following diagram published in the original Technical Whitepaper, provides a clear delineation of the Blockstack architecture.

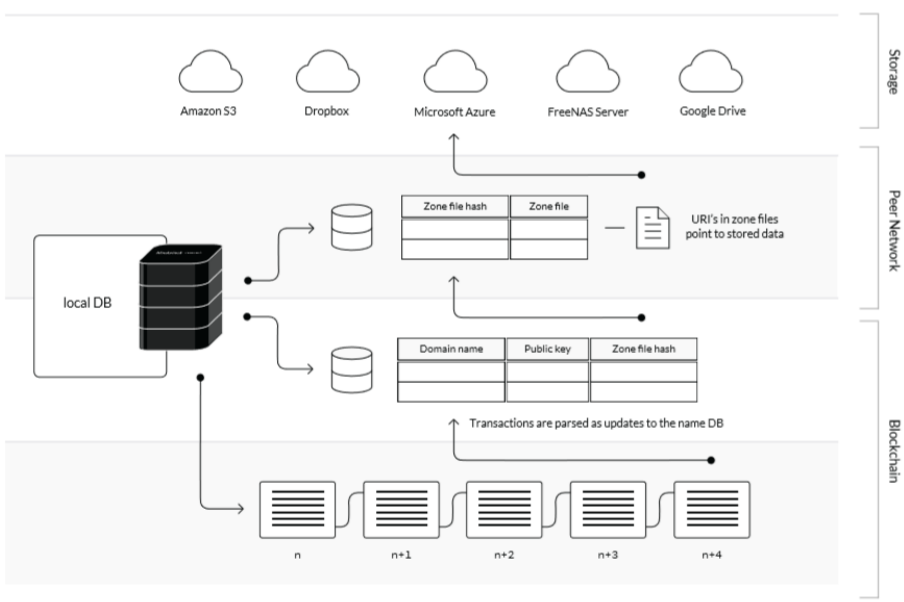

Figure 1: *Overview of the Blockstack architecture.*

Source: https://blockstack.org/whitepaper.pdf

These three architectural layers can be further delineated between a control plane (blockchain) and a data plane (peer network and storage). The blockchain is the lower layer as serves two purposes according to the blockstack Whitepaper, to provide the storage medium for operations and the consensus in the order in which operations were written. Virtualchains sit above the blockchain and encodes operations in the blockchain. The peer network layer in Blockstack is called Atlas and provides a global index for discovery services. The storage layer in Blockstack is called Gaia, and provides a decentralized storage system using existing services providers without the need for any centralized trust providers.

To date there have been over 75,000 names registered in Blockstack, and in May 2017 Blockstack released a browser plug that permits developers to begin creating applications using the Blockstack protocol. Blockstack has followed a more traditional VC path raising an initial 5.45 million in 2013, and then an additional 25 million in 2017. However, Blockstack is currently preparing for an Initial Coin Offering (ICO) that is scheduled for 1 November 2017.

Patent Filings

There are several objective metrics to gauge the growing global interest in DLT/blockchain technology ranging for capital investment, news coverage, to work within various international standards bodies. However, one of the more interesting metrics is patent filing, in particular, filings by existing ICANN community members. Bill Manning was one of the first ICANN community members to file a patent application with the United States Patent Office (USPTO) in June 2016 for an "out-of-band Domain Name System (DNS) security technique uses a cryptographic blockchain for securing and validating DNS data in a chain of custody that exists outside the DNS namespace, allowing validated access to cached DNS information without requiring real-time access to root servers."[3]

Perhaps more interesting is a series of three recent patent applications filed by VeriSign in 2017 with the USPTO.[4] This portfolio of patents all deal with extending DNSSEC trust chains to objects outside the DNS, and all three specifically reference the potential embodiment "utiliz[ing] public ledgers and blockchains." Further insight into the potential scope of VeriSign's is set forth is set forth in the abstract which reference "the ability to validate a chain of trust starting with the trust anchor at the DNS root all the way to a service or object of interest outside the DNS." The specific inclusion of the word "object" implies potential Internet of Thing (IoT) deployments.

Other International Fora

There are several international bodies that are closely evaluating DLT/blockchain technologies at the current time. The W3C's has several blockchain interest groups including the Verifiable Claims Working Group that is evaluating a new format for interoperable digital credentials utilizing DLT/blockchain technologies. The International Organization for Standards (ISO) is currently evaluating potential standardization of blockchain technologies and distributed ledger technologies in ISO/TC-307. ISOC, consistent with its mission to "promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world", recently created a Blockchain Special Interest Group to begin analyzing blockchain's potential broader impact.

There are also several initiatives within the United Nations that are looking at DLT/blockchain technology, although the International Telecommunication Union (ITU) has been the most active by far. The ITU activities in this area include: SG-17 that held a workshop on Security Aspects of Blockchain in

[3] Patent Application - 20160191243
[4] Patent Applications: 20170012780; 20170012943 and 20170310484

March 2017; the establishment of a focus group on the application of distributed ledger technology (FG DLT); and the proposed fast tracking of blockchain protocols regarding financial transactions. In addition, a group of Chinese companies including China Unicom, ZTE and Alibaba Group recently joined with the Egyptian National Telecom Regulatory Authority in submitting a paper to the ITU's Internet of Things (IoT) Study Group. This paper, entitled 'Framework of blockchain of things as decentralized service platform', recognizes how blockchain can provide a unique framework for the future growth and evolution of the IoT.

ICANN at Organization Crossroad

I have been deeply involved with ICANN since its creation in 1998, and over the last decade I have had the opportunity to work with numerous Inter-Governmental Agencies on various internet governance related projects. During this time, I have had the benefit of seeing first-hand the strengths and weakness of each model up close and personal. Historically, one of the strengths of the ICANN private sector lead model was its ability to quickly react to market dynamics, whereas the Inter-Governmental model was perceived as a more slow and steady process broken down into four-year cycles coinciding with the election of leadership. Unfortunately, ICANN's current bottom up consensus driven model has resulted in an almost organizational paralysis where divergent economic and philosophical differences of its various stakeholders prevent any substantive policy change and/or innovation in a timely manner.

There is probably no clearer evidence of this paralysis than to look at the how ICANN has handled the roll out of new gTLDs. In May of 1999 at its regional meeting in Berlin, ICANN created Working Group C to make policy recommendations regarding new top-level domains. In July 2000 at its Yokohama meeting, the ICANN Board approved a new gTLD proof of concept round based on the recommendations of the DNSO, the predecessor of the GNSO. In August 2000, ICANN published instructions for prospective registry operators to submit their applications. Applications were accepted by ICANN beginning in September and the ICANN Board approved seven proof of concept TLDs a mere two months later in November of 2000. A total of four months elapsed from the period when the ICANN Board approving a new round of TLDs and them selecting the seven registry operators to enter into contractual negotiations with ICANN.

In July 2011 at its regional meeting in Singapore, the ICANN Board approved a final Applicant Guidebook for new TLDs. ICANN began accepting applications in January of 2012 and were originally supposed to close the application round on April 12th prior to an unforeseen glitch that pushed closure to June. ICANN then signed its first new registry agreements in July 2013. Despite the original Applicant Guidebook stating that "[t]he goal is for the next application round to begin within one year of the close of the application submission period for the initial round," ICANN's current best guess on the earliest for when the next round of new TLDs will open is 2020.

Another example of ICANN's paralysis with potential more dire consequences is the issue of Whois access and data privacy. This is an issue which has been more thoroughly contested in ICANN's 18 years history than perhaps any other. However, the pending enforcement of the GDPR's provision in May 2018 has resulted in ICANN and its contracting parties being caught flat footed and now playing a very dangerous game of catch-up. Sadly most of the banks that acquired a .BRAND TLD in the 2012 round have done nothing of substance with them, while they have invested millions into various DLT/blockchain trials and proof of concepts. The impact that DLT/blockchain will have on the broader internet eco-system is not a matter of if, but when. Therefore, it is important to know what ICANN's policy on this technology is and how it will respond when registration authorities being integrating this technology into the existing Internet infrastructure.

Conclusion

In 2016, the great ICANN experiment in bottom up multi-stakeholder internet governance took an important step forward with the complete and free transition of the IANA functions from the United States Government. This is an important accomplishment that needs to be acknowledged and celebrated by all ICANN stakeholders that made it possible. However, this accomplishment did not represent the end, but a next step in its continuing journey to reinforce and validate the multi-stakeholder model.

As noted above ICANN has reached an interesting inflection point in its own organization evolution, where the economic interests of certain stakeholder can hold certain processes and the organization itself hostage. ICANN's original general counsel, Louie Touton, once wisely stated that ICANN's mission is to protect competition, not individual competitors. DLT and blockchain technologies are disruptive technologies that will upset existing business models. The challenge for ICANN is whether it will welcome and embrace this technology, shun it, or perhaps worst, lets it languish in a perpetual Working Group purgatory. Hopefully ICANN will choose the right path, because the rest of the world is NOT idly sitting by on the sidelines with respect to this exciting technology.