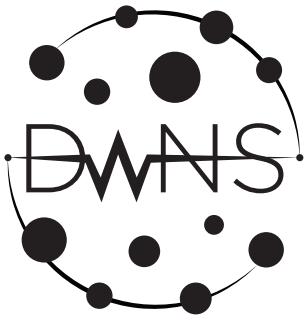


DwNS

Secure, anonymous and unblockable name system.

8.3.18

"Concentrated power is not rendered harmless by the good intentions of those who create it."

- Milton Friedman

Join Telegram Group: https://t.me/dwnsofficial
or email: info@dwns.io

ABSTRACT

We aim to create a decentralized autonomous organization (DAO) that will replace the aging DNS system and change the economics of domain ownership. Only by incubating a DAO Registrar with its own token system can we create a lasting and self-sustaining economy that can replace ICANN. This ability to remove people and governments from the central control of the Internet is a must to the development of a permanent uncensored internet. Currently, the web is under the de facto control of ICANN, a non-profit organization, and all of the top level domains (TLDs) such as .com and .io are chosen and controlled by ICANN. ICANN then delegates the TLDs to one or more registrars like GoDaddy. GoDaddy then has wide latitude to create their own Terms of Service. Recently some registrars have revoked domain registrations due to violations of those terms of service.

The age of Internet censorship is now upon us. What was once free and open has now become a heavily regulated over scrutinized censorship machine. Power has consolidated into the hands of Facebook, Google, and Twitter. As they seek to stay on the right side of politicians and regulators, they offer up our freedoms like cheap carnival prizes. Their jobs are made nearly impossible due to the sheer vitriol and animosity on both sides of any issue these days. The next step will likely become extreme government regulation like China, Iran, Turkey, and Russia have adopted.

In addition to censorship major corporations are now controlling vast amounts of personal data. Massive data breaches including 3 billion records from Yahoo! in December 2016, 145 million records from Equifax in December 2017 and 110 million records from Target in November of 2013 are regularly occurring. The public is becoming aware that they need to have greater control of their data, which means the need for a new, more decentralized and anonymous internet. The existing infrastructure was not designed to allow for this. We believe that the decentralized web name system is a necessary starting point to fill this void. People need to be able to find resources within the new decentralized internet that is forming, and they will demand that the naming system remains decentralized.

We believe the proper combination of blockchain technologies and P2P networks can create a system similar to ICANN without the arbitrary control and fallacies of humankind. It can be fault tolerant and censorship-resistant.

However, there is no point in taking the existing system and just putting it on a blockchain. DwNS isn't merely DNS on a blockchain, it is a better naming system. We looked at where the current system was lacking and what it could look like if it weren't held back by legacy technology. We built DwNS to be the name system the brave new internet needs and deserves.

DEFINITIONS

DwNS
Decentralized web name system - the topic of this paper

DAO Registrar
A naming registrar that functions as a decentralized autonomous organization

TLD
Top level domain in the current domain name system, for example ".com"

FQN
Fully qualified name, the label for the zone plus all of its parents, for example fantasy.sports.

Zone
A name in the new DwNS. There can be many sub-zones under a parent zone. A sub-zone is similar to a subdomain in the current domain name system.

TLZ
Top Level Zone - this is a zone that is directly under the root zone. For example "sports" can be a TLZ and "fantasy.sports" represents a sub-zone of "fantasy" under the parent or TLZ "sports."

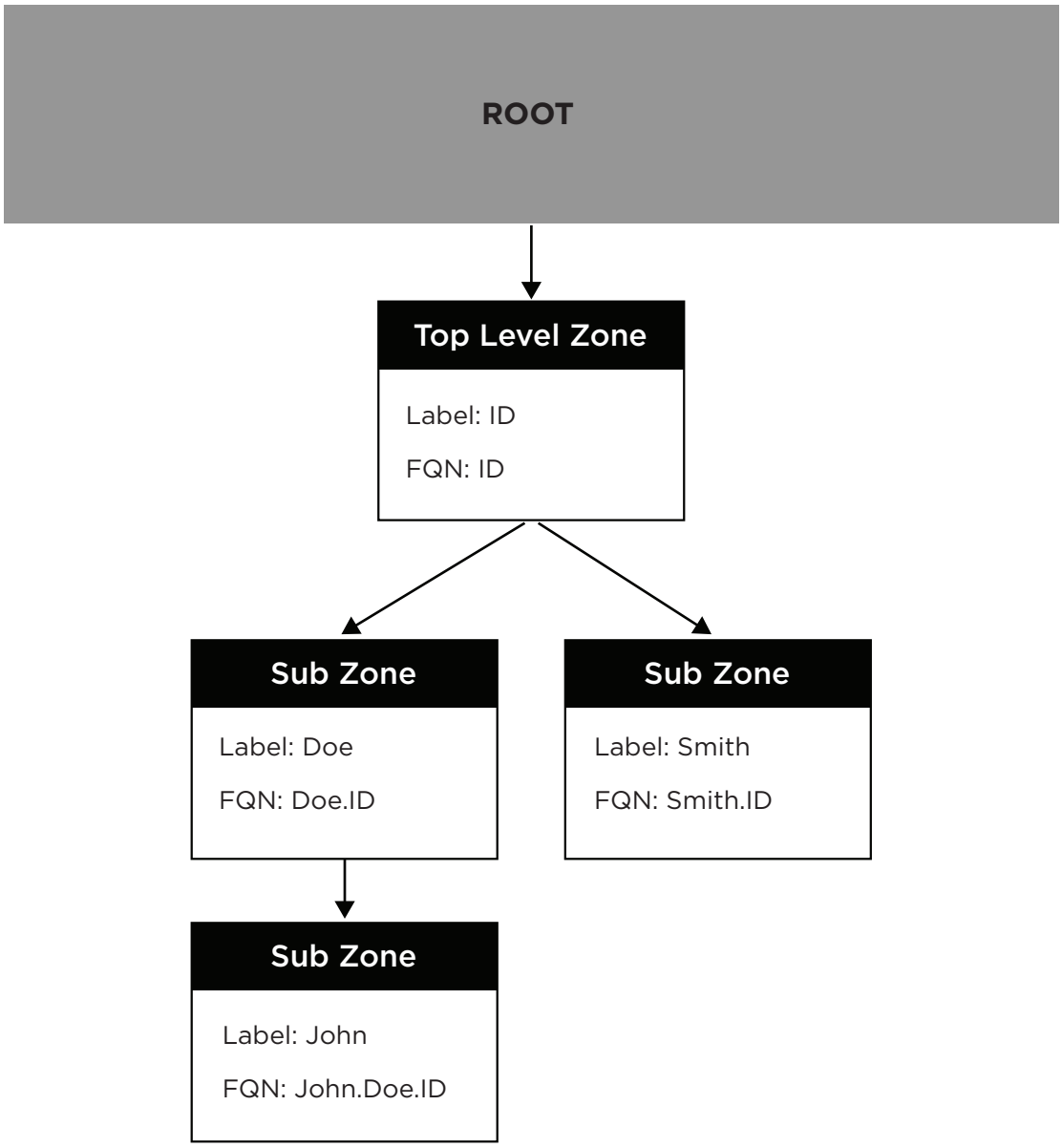
ERC-721
An Ethereum contract for non-fungible tokens, each ERC-721 token represents a single name, aka a zone.

IPFS
InterPlanetary File System (ipfs.io)

ERC-223
An Ethereum contract for fungible tokens. In DwNS these tokens are burned to create sub-zones for the zone they belong to.

This diagram illustrates the naming conventions used in this paper.

The following diagram illustrates the naming conventions used in this paper. The system starts with a nameless Root Zone. A top-level zone (TLZ) is the beginning of a fully qualified name (FQN) in DwNS. All TLZs are sub-zones of the Root Zone. Sub-zones can be created under the TLZ, and a sub-zone can have sub-zones of their own and so on. The FQN is defined as the combinations of zone labels, with the TLZ label being the furthest to the right.



PROBLEM

Censorship is a daily reality for many Internet users. Workplaces, schools, and governments use technical and social means to prevent access to information by the network users under their control. The DNS system is fraught with vulnerabilities. The biggest weakness in tightly controlled networks is the fact that state actors can control access to DNS servers. With 100% control over DNS servers, censored websites can have their URL's, and associated IP addresses deleted, modified or rendered to non-sensical sites.

The Internet was designed to be fault tolerant from a network perspective, but the current naming scheme we use is massively centralized and subject to government interference. China controls every DNS server located in mainland China. They control with 100% certainty how websites are resolved for 1.4 billion people.

In the current system, you do not own your domain name you are leasing it and must continuously pay to maintain your rights to use the name. Because you do not own it, the domain name can be taken back at any time or shut down by a government. For example, the FBI seizes websites and shuts them down on a regular basis. Your domain name is administered by a registrar, which are subject to contracts with ICANN and the laws and regulations of the countries they operate in.

The current DNS is also susceptible to DNS cache poisoning attacks, a recent example being myetherwallet.com which was redirected to a hacker's website to collect private keys and other valuable information, through an attack on one of Amazon's popular DNS servers.

Finally one has limited options when getting a website domain name. You can only choose from top-level domain extensions that ICANN has released and made available to registrars. Selling off subdomains while possible is rarely done and difficult to monetize. Only 7 non-geographical TLDs predate the creation of ICANN in 1998. Even with the additional TLDs that are now available, it is still a small number of choices, and the actual domain names are restricted to a subset of ASCII text.

SOLUTION

We propose a decentralized, blockchain based, solution to replace current DNS servers. Zones ownership and creation is managed by a combination of Ethereum ERC-721 and ERC-223 tokens. Zone data will be stored in IPFS, Bitcoin Cash, Distributed Hash Tables(DHTs) or any future technology capable of running in a decentralized manner. The solution is modular and upgradable to allow for future growth and new ideas. We will be able to replicate the current DNS system in a decentralized manner while enhancing it at the same time. The system will function as a DAO Registrar with no human control, governmental or otherwise.

By using a very large public blockchain, a government body would need to attack Ethereum or Bitcoin Cash and cause massive collateral damage. With the amount of money at stake, this would hurt the attacking country and citizens of other nations forcing a response. Case in point: a lot of services reside on CDNs, and the Chinese govt has been leary to go after specific assets on those CDNs because of the collateral damage they would cause for the access to other sites also hosted on those same CDNs.

USE CASES

Censorship: When a website is continually being blocked by a hostile state actor, the users have to learn about the new website URL on a daily basis to maintain access to the site. The online company purchases the zone with the FQN “xyz.info” from a DwNS auction and now owns it for all time. Their users can now consistently access the blocked website using the DwNS browser extension by typing in the same value “xyz.info” every time.

Global identification: A user obtains their DwNS zone with a fully qualified name of john.smith.id. This FQN becomes their global identify and can be used through the DwNS browser extension to access their website, their Twitter account, their LinkedIn profile, etc. Their FQN can be used by others to securely message them in a way that cannot be censored. The user can record wallet addresses in the zone for different cryptocurrencies allowing digital assets to be sent to a human-readable FQN instead of an incoherent address.

Token ecosystem: A sub-zone can be acquired underneath a parent zone. This sub-zone can be locked to prevent new sub-zones from being created under it. The owner can then run their own ICO with the supply of ERC-223 tokens assigned to that zone. These tokens can be generated for any zone with no coding or contracts needed. The token is directly associated with a zone in DwNS, so it is easily searchable and usable by zone name. This naming convention for token issuance allows for searching, listing sites, and allows a token to be automatically added to wallets.

Gaming: A company obtains the zone tradingcard.sports and therefore has all of the utility tokens for that zone. Those tokens can be sold to game players to create a sub-zone for each athlete, for example, tombrady.tradingcard.sports. There will be a single owner of each player’s non-fungible token that can be sold or traded for other players. The player’s sub-zone can be used to access stats and additional information about that athlete, or used as an asset in an online sports game. These trading cards can seamlessly integrate with other smart contracts and create whole new ecosystems and economies. This use case shows how DwNS is so much more than a naming system.

Github: The recent purchase of Github by Microsoft has revealed yet another excellent use of DwNS. Git itself was designed to be decentralized, but developers need a way to discover and manage open source code. In a client-server environment with centralized control naming repositories of code was a simple task. Wikipedia reports that as of June 2018, GitHub reports having almost 28 million users and 57 million repositories, making it the largest host of source code in the world. Use cases like this abound, and the massive number of TLZ and sub-zones is easy to understand. We intend to release .repo as one of the first TLZs and quickly integrate a Git implementation. If only a small fraction of the 57 million repositories run on DwNS, the .repo TLZ will be extremely valuable.

DIFFERENTIATORS

Decentralized: This new system is not easily blocked by a government entity, and it does not serve the interest of any single party. No longer will governments be able to go to registrars or hosting data centers and shut down websites.

True Ownership: When you acquire a TLZ or a sub-zone, you own it and can prove ownership via your non-fungible ERC-721 token. It isn't a lease like current domains. You can then trade, sell, or auction your zone asset, and do the same with the ERC-223 tokens that allow for the creation of sub-zones under your zone.

More domain name options: One can buy and sell at all levels of a zone, not just at the top level. Each TLZ has associated ERC-223 tokens which allow the creation of sub-zones under that TLZ. These tokens will be auctioned off for each TLZ created during the incubation phase enabling purchasers to claim their own piece of that TLZ. For example, when the .repo TLZ is released an auction will be held that will allow a developer to purchase the tokens needed to claim the myproject.repo zone.

Frequent Releases: We will release TLZs much more frequently than ICANN released their top level domain names (they only had about 7 for decades). We intend to structure the release for an initial period of time while the DOA is being incubated then open up the system so anyone can create a TLZ.

Multiple Uses For Domain: A single zone name entry created in DwNS can be used to access much more than just a website. For example, a person's domain address can be used to send them Ethereum, message them, go to their LinkedIn profile or read their Twitter feed. DwNS will seamlessly integrate with IPFS and owners of zones will be able to point those zones to IPFS hosted sites for a completely decentralized system. Our initial integration with IPFS and Git is intended to show the power of DwNS. As the world realizes that the decentralization of the Internet is a necessity, it will also recognize that a decentralized naming schema is a necessity as well.

Non-ASCII: We propose a system not limited to ASCII characters. While possible to use foreign languages to register domain names using conversion tools, it is more difficult than it needs to be. Zones in DwNS will include Emojis, foreign language characters, and any Unicode character minus a handful of reserved characters used for encoding. That is over 1 million potential characters, and over 100,000 already assigned characters. The current DNS was developed using old technology that is limited in light of current technology. So much of the internet runs on this old system people are hesitant to change and creating consensus is nearly impossible.

BUSINESS MODEL/ECONOMICS

The genesis of the DAO Registrar is a "root" ERC-721 contract and a fixed number of "root" ERC-223 tokens that are used to create the TLZ such as sports, business, token, etc. DwNS, LLC will retain ownership of these root ERC-223 tokens while the system is incubated and will then sell off these tokens so that others can create top-level zones.

During the incubation period DwNS, LLC will be burning "root" tokens to create TLZs and then auctioning off the ERC-223 zone tokens for each of these TLZs. DwNS, LLC will retain ownership of each TLZ ERC-721 token during the incubation period as well and will then sell each ERC-721 token off, thus transferring ownership of TLZs to others. The sale of TLZs will be performed using a reverse clock auction (see below). This will further strengthen the DwNS economy. The final step to transfer ownership of the entire system to the general public will be for DwNS, LLC to auction off the root ERC-223 tokens to enable others to create their own TLZs. Proceeds from all sales The default sales process will start with a Dutch Auction where we auction off 60% of the total available tokens. Each person that contributes Ether during the auction will get a percentage of the ERC-223 tokens in relation to the percentage of Ether that they contributed.

By example:

1,000,000 tokens are being auctioned off for the TLZ .sports. Over the course of two weeks, bidders send Ether to the auction contract. At the end of the two weeks, each bidder's contributed amount is divided by the total Ether collected. In this case, let's assume our bidder contributed 25 Ether out of a total of 500 Ether contributed by all bidders. Our bidder would now receive 5% of the ERC-223 tokens that were auctioned (25/500 = 5%). The formula for this is:

Ether contributed by Bidder / Total Ether contributed = % Tokens Received by a Bidder.

In this example, the bidder receives 50,000 tokens, which is 5% of the 1,000,000 tokens auctioned. Stated another way the bidder received 2000 tokens per Ether (50,000 tokens for 25 Ether contributed).

After the auction closes the new owners of the ERC-223 token will now be able to register sub-zones for a to be determined number of parent ERC-223 tokens per sub-zone. The first person to register a sub-zone acquires it. By example, a token owner must burn 1000 tokens to register "fantasy" under the "sports" TLZ. People using the system will be able to access their sub-zone by typing in "fantasy.sports" or "fantasy sports" in one of the DwNS clients such as a browser extension and manage the zone in the registrar software.

A person registers the "fantasy" sub-zone by burning a preset number of "sports" ERC-223 tokens. The "fantasy" sub-zone is now irrevocably associated with a specific non-fungible ERC-721 token that the person who registered it owns. The owner can now create their own supply of ERC-223 tokens associated with the "fantasy" sub-zone. The owner can then create their own economy around the "fantasy.sports" name. These ERC-223 tokens are fungible utility tokens that have many potential use cases for the owner's economy. Here are a few examples.

People using DwNS will land at the owner's website and other resources when navigating to "fantasy.sports".

The owner can auction or sell sub-zones (aka subdomains), for example "nfl.fantasy.sports".

The owner can use his tokens to offer an ICO that revolves around the owner's specific namespace. For example the "fantasy.sports" ICO.

Decreasing Cost of Sub Zones

The number of parent ERC-223 tokens required to purchase a sub-zone will gradually lower; for example, it decreases by 100 tokens per month. This decrease is also reflected in the amount of Ether required to buy a sub-zone directly. Using this process the highest value sub-zones are acquired first at a higher cost, and then people are still incentivized to purchase lower valued sub-zones. This approach also keeps people from buying up sub-zones in bulk.

Buy Now (40% of total supply)

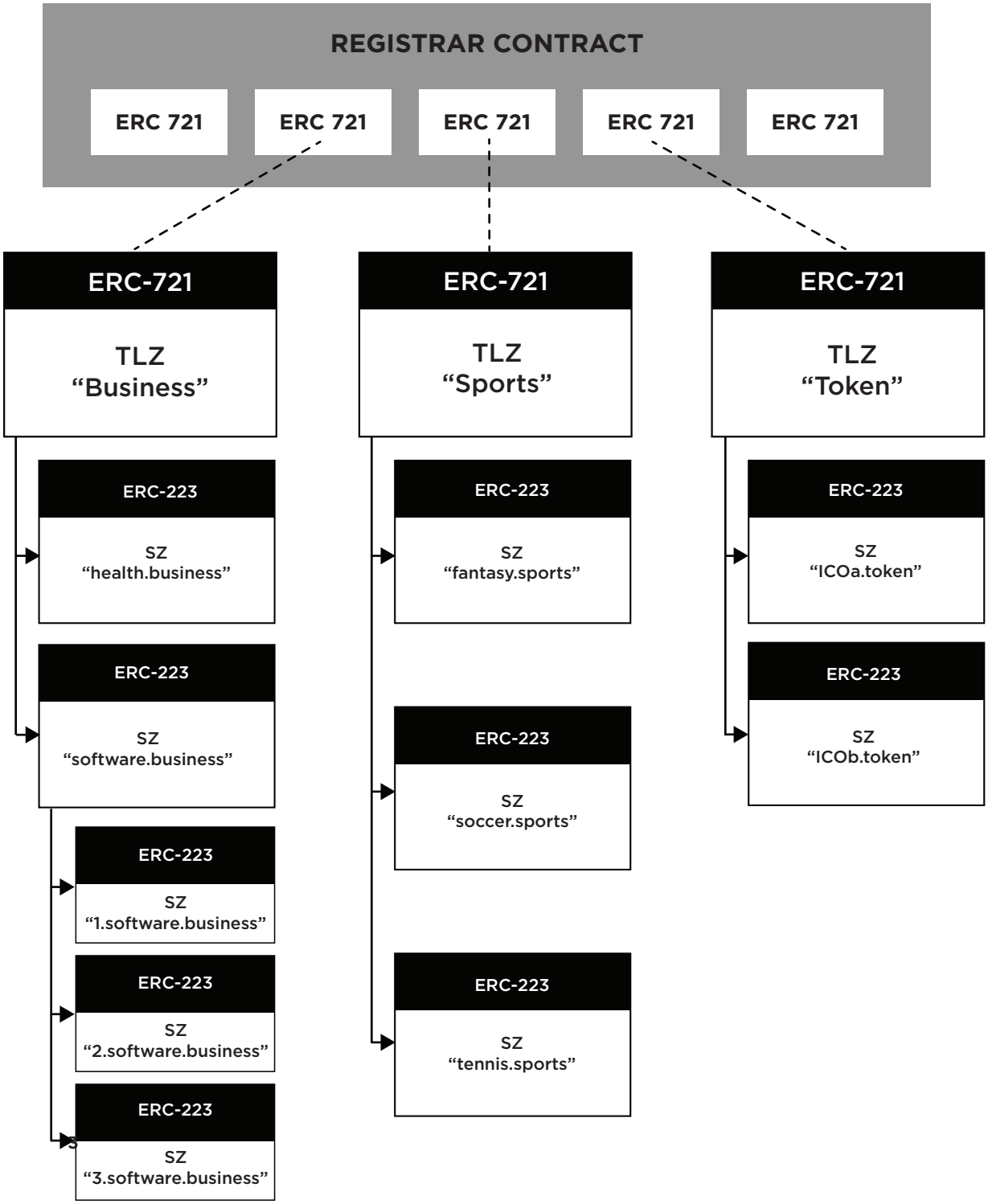
Two weeks after the auction ends we will offer a "Buy Now" function to allow people to purchase ERC-223 tokens. 40% of the total number of the zone's ERC-223 tokens are reserved for this purpose. There is a 25% markup based on the price per token at the end of the auction. This is an incentive for people to participate in the auction. Therefore someone purchasing tokens at the end of the auction will have to pay 1.25 Ether to receive 2000 tokens if the ending auction price was 1 Ether per 2000 tokens. Once someone has performed a "buy now" to buy ERC-223 tokens, they can then burn the current required amount of those tokens to acquire a sub-zone immediately. Note that the registrar UI may hide this additional step of purchasing tokens and merely show the cost in Ether to buy a sub-zone.

Auctioning a Zone (ERC-721 ownership):

The ERC-721 top-level zone is sold using a reverse clock auction that is defined and controlled via an Ethereum smart contract. We give credit to Crypto Kitties for bringing to light the benefits of non-fungible ERC-721 contracts, their usefulness, as well as the reverse clock auction. A maximum start price, minimum end price, and auction time are set, and then the sale of the TLZ begins. The price (in Ether) of the TLZ starts at the maximum price and ticks down to the minimum price over the time range allocated for the auction. The first person to purchase the TLZ gains full ownership of the ERC-721 token. That person can then choose to sell or auction off some or all of the associated ERC-223 tokens linked to that zone. The ERC-721 owner can trade, sell, or auction the token at any time transferring ownership of that zone.

non-fungible ERC-721 contracts and their usefulness. A maximum start price, minimum end price, and auction time are set and then the sale of the TLZ begins. The price (in Ether) of the TLZ starts at the maximum price and ticks down to the minimum price over the time range alloted for the auction. The first person to purchase the TLZ gains full ownership of the ERC-721 token. That person can then choose to sell or auction off some or all of the associated ERC-20 tokens. In addition the TLZ owner can keep them for himself or not create any. The ERC-721 owner can trade or sell the token at any time transferring ownership of that zone.

The diagram below shows an example of the hierarchy from the root registrar contract to each top level zone (TLZ) and then downwards to sub-zones.



ARCHITECTURE

The decentralized web name system (DwNS) uses Ethereum contracts and tokens to track web name ownership. The term "zone" is used to represent a single name in the system. Each zone except the root zone has a parent, and the zone hierarchy forms a name or path to retrieve that zone's resources. This is analogous to domains and subdomains in a traditional DNS system, except that it can extend. For example a web name of nfl.fantasy.sports, "nfl" is a sub-zone of "fantasy", which is, in turn, a sub-zone of the top level "sports" zone.

Each zone is represented by a non-fungible token in an ERC-721 contract, meaning there is only ever one ERC-721 token on the public Ethereum blockchain for a specific zone. The ERC-721 contract contains the information for a zone, and it maintains the hierarchy between zones. A set of ERC-223 tokens can be created for each new zone. The ERC-223 tokens are then used to establish value within that zone. This means that owners of the ERC-223 tokens may have the ability to create a sub-zone by burning some or all of their tokens if the parent is configured to allow for that. Otherwise, someone acquires the tokens because the owner of the zone has established some other type of value for that zone, such as an ICO.

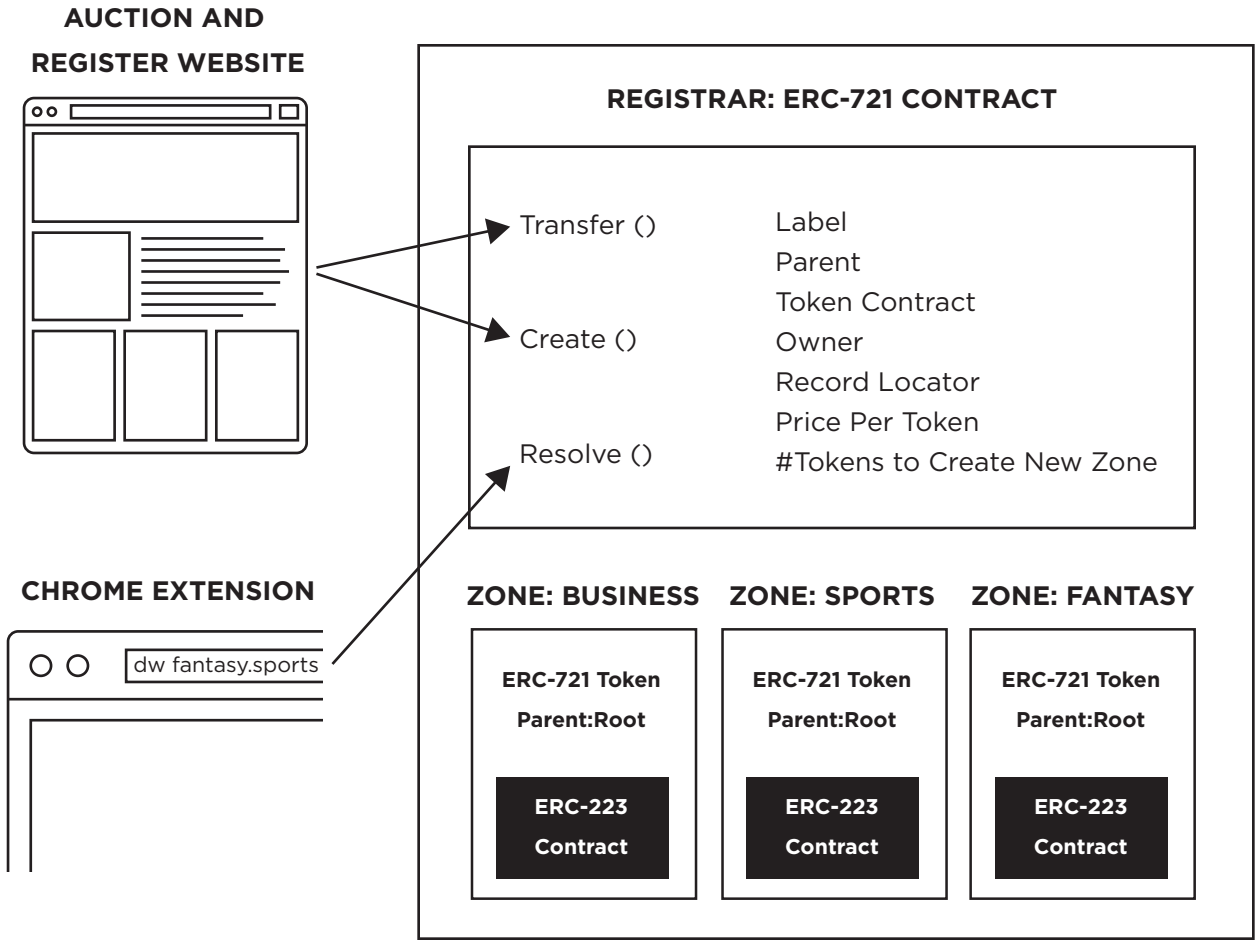


Figure 3

Figure 3: ERC-721 Contract and Token Layout

The primary values that get stored in each ERC-721 token are:

Label: the zone name (ex: "fantasy")

Parent: the parent zone (ex: "sports")

Token Contract: a pointer to the ERC-223 contract specific to this zone

Owner: the Ethereum public key representing the owner of this token/zone

Record: a type and pointer used to lookup the data for the zone

Price: the cost in Ether for each ERC-223 token

 # Tokens to create new: the number of ERC-223 tokens that must be burned to create a sub-zone

The required methods for the DwNS ERC-223 contract is shown in the figure below. A burn method is added to dispose of ERC-223 tokens for a specific zone when those tokens are used to purchase a sub-zone. The registrarAddress field is a pointer to the registrar's Ethereum contract; this is used to facilitate the burn functionality.

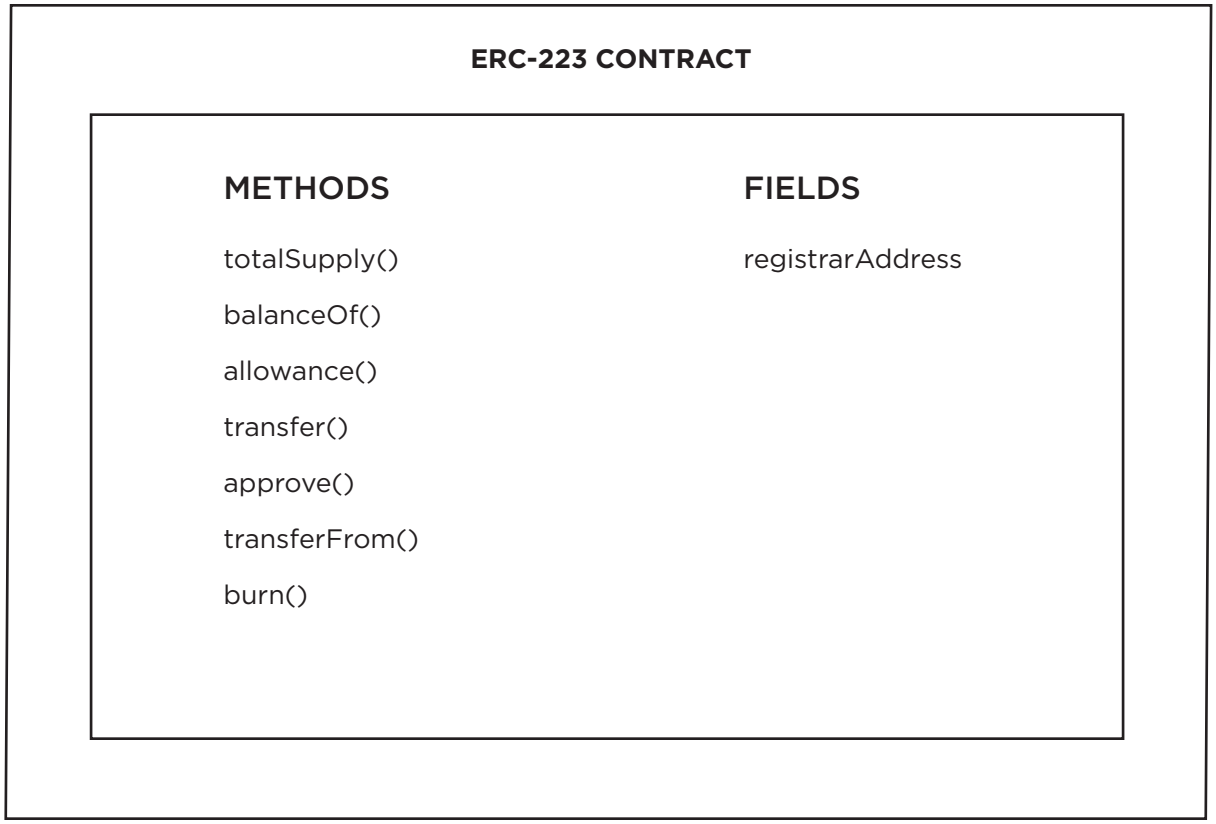


Figure 4 : ERC-223 Contract

The system starts with a root zone that DwNS, LLC owns. Top level zones (TLZ) are created from there by burning root ERC-223 tokens. The ERC-223 tokens for the TLZ are then sold or auctioned off to anyone that wants the ability to create a sub-zones under the TLZ. This is essentially the same as creating a subdomain in a traditional DNS system, with a fundamental difference being that multiple parties that own the parent zone ERC-223 tokens can create sub-zones even though the parent zone has a single owner. This parent/child relationship continues downward indefinitely. For example, a sub-zone called "company1" could be created under the parent zone "software" which in turn has a parent TLZ "business", representing a fully qualified name of "company1.software.business", which could be used in the DwNS browser extension and other supported clients to reach the "company1" website.

Each zone points to a data store to hold information about that zone. Initially, the most common type of data will be ipv4 and ipv6 values for the zone, to point at the website for that zone. These IP address values may never be updated after zone creation, or they might be updated daily to get around continual IP blocking from a government that is censoring the website. Any type of data can be stored for a zone, another example is a pointer to an IPFS folder containing HTML and javascript files. This would allow the decentralized web name system to fetch static website content and render it without going to any centralized web server. The supported data stores that will initially be supported are:

IPFS: A globally decentralized file storage system. Every time the data is changed there is a cost to then update the ERC-721 contract. This is because the lookup key in IPFS is a hash of the data. Changing the data changes the hash which then needs updating in the contract. This store allows for large amounts of data to be easily stored, for example, to host an entire static website. A hash of the IPFS data is used as the Record Key.

BCH: The public BitCoin Cash blockchain. Since the BCH public address is used as the Record Key, the ERC-721 contract does not need to change when data is changed at the BCH address, making this a cheaper option and more ideal for a constantly changing IP address. The only cost is the BCH transaction fee to update the data. We have picked Bitcoin Cash over Bitcoin Legacy due to the larger available data limits in blocks and the lower transaction fees.

Functions in the ERC-721 contract:

Transfer: Transfers ownership of the ERC-721 token from one Ethereum public key to another.

Register: Creates an ERC-721 token and sets the zone fields to configure it. The Register function in the smart contract will be called from the Registrar website when a user registers a new zone. The registrar checks that the owner has enough of the ERC-223 token and then burns it as part of the registration process.

Resolve: Uses the FQN to find the data store and to retrieve information about how to connect the client to the zone resource. This could be an IP address pointing at a centralized website, or it could be a pointer into an IPFS folder that contains an index.html and all dependent resources to launch a decentralized website.

The Auction website will execute the rules defined in the auction smart contract to auction off a zone's ERC-223 tokens. This includes distributing ERC-223 tokens to each participant based on the amount of Ether that they contributed.

Multiple clients will be created for easy access into the DwNS:

Browser extension: Allows users to browse using the new zone names and will also support loading apps that are fully stored in IPFS. The user will have to type in a keyword in the address bar such as “dw” to signify that they are browsing the new decentralized system.

Dedicated browser: A separate browser install that will always use the DwNS and will therefore not require a keyword to be specified.

DNS Server: a special DNS server will serve as a bridge into the decentralized web name system. A client OS can be configured to point at our server or a locally hosted DNS server, which will behave like a traditional DNS server. It will first look up the name that is being requested within the DwNS system, and if not found it will look up the name as a traditional domain name on the internet. This client will be limited to names allowed by the current DNS system and as meant to make for an easier transition.