butterflyprotocol.io

WHITE PAPER

Table of Contents

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.

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 finally 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.

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 is in demand. 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. Butterfly 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 Butterfly to be the name system the brave new internet needs and deserves.

Introduction – Market Overview

The moment a website address is entered into the browser, the computer automatically requests a Domain Name System (DNS) server to convert that request to a numerical value (i.e. 987.654.321.00), which, as a result, displays the website being requested for. Regrettably, these DNS servers are under total government jurisdiction, giving them the power to determine whether DNS requests should be undertaken or ignored. Even though this technique, known as centralized DNS, yields higher dependability and authenticity, it tolerates a substantial amount of government censorship, which is audaciously misemployed by exploitative countries.

To make things even worse, on top of authoritarian government institutions using this approach to limit the people from voicing their thoughts, any government body can decide to put down any website, independent from their actions – legal or not. Simply put, governments can pull the plug of any "hostile" website, thereby further restricting the already depleting freedom of expression.

It would hardly be far-fetched to state that many of today's online users take Internet and online presence for granted with how easy it is to create a website for personal or corporate use. With the Internet as accessible as it has ever been, anyone can join the online community, either as a user or an operator. It is all too understandable as well with how effortless it is to acquire a domain name in minutes and set up an online page.

Worth well over $4 billion and with more than 300 million websites, the Domain Naming industry is continuing to grow, but few realize how centralized it is.

It all stems from ICANN, who is solely responsible for distributing Top-Level Domains such as .com, .net, .org etc. extensions to name a few. The major domain name registrars GoDaddy, Bluehost, Hostgator, Namecheap and a few others have a firm grip on that domain name extensions that are offered, monopolizing the market with continuous renewal costs and limited domain name availability.

Butterfly is here to bring the future of Internet domain name creation, acquisition and ownership – one with a decentralized nature, where individuals and enterprises are able to select a domain name that uniquely identifies them on the new internet, without having to stay within the current DNS restrictions of a limited set of top level domain name extensions, thanks to blockchain technology.

While decentralized domain naming systems have been developing for a while, only a few match and address the industry's challenges as thoroughly as Butterfly. Domain name owners have their domain infinitely, free of renewal costs, while the network employs a proprietary web-browsing extension to counter censorship and content blocking.

Butterfly also aims at opening up economies under every domain name by streamlining the old-fashioned process. Therefore, each domain address can be employed for a plethora of functionalities such as Ethereum transactions, messaging, social media managing, etc. Butterfly will seamlessly integrate with IPFS and owners of domains will be able to point those domains to IPFS hosted sites for a completely decentralized system. Our initial integration with IPFS and Git is intended to show the power of Butterfly. 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.

The Butterfly Protocol enables individuals to suggest, sponsor and bid on the creation of new domain names and then receive a share of the tokens associated with that domain. The individual can then leverage those tokens to create subdomains, thus opening up endless new economies.

Problems

Currently, state authorities and governing, regulatory bodies are in power to block and/or delete any online content they deem inapt. This is a major barrier in the current state of the Internet - when it comes to free access to information and concerns numerous industries, with one of them being media outlets, for example. No matter if we are talking about a social media channel, a major news portal, a niche investigative journalism website or a simple personal blog post page - governing officials in autocratic states have the ability to single-handedly block specific domains, so publishers are powerless in getting quality content to reach an interested audience.

The current state of domain names remains dormant as the registrars, in the face of market-monopolizing corporations, never actually sell the domain name, but merely lease it to customers for a time period. This is why one has to renew the domain name they have personally acquired on an annual basis. This creates more issues in the face of domain-name parking, which itself creates space for speculation and brokering practices, all of which create inefficiencies. For instance, one might have been quick enough to snap up their perfect domain name but has somehow missed renewing it, which in turn would ruin their online presence as numerous brokers are constantly scouting for expired, sought-after domains, acquiring and selling them at a premium. While a business model in itself, this adds little to no value for what Internet domain name ownership is meant to be.

Similarly, one of the major issues is the limited domain name extension availability, imposed by ICANN (Internet Corporation for Assigned Names and Numbers). This US-based non-profit organization has not been addressing Internet users' and domain owners' needs enough when it comes to domain name selection – only a handful of top level domain name extensions were available for many years, and some of those were restricted like .edu, .mil, .gov. This has severely limited opportunities of both personal and corporate Internet usage. As an example, suppose that someone operates a car rental business. It would be impossible under the current state of domain name registering to acquire carrentals.com, simply because it is either already taken and in operation or because it is valued, accordingly, at a vast amount of a purchase price. Ultimately, the same domain and all its subsidiaries would be owned by a single entity, thereby restricting any inclusions from other participants.

Another reason the current Domain Name System is regarded as legacy technology comes from the limitation of characters available for the actual names of the domains and associated extensions. Current domain names can only contains the characters a-z, 0-9, and hyphens. The Butterfly Protocol opens up the use of most Unicode characters including symbols for Asian languages and even emojis. The example below is for the Chinese car manufacturer BYD Auto. It shows that one could create a domain name with a mix of emojis and Asian characters.

比亚迪汽车.🇨🇳.🚗

As mentioned earlier, it cannot be denied that the existing Domain Name System has created a specific business model in the face of domain name parking. Individuals are free to acquire a TLD, with no intent to utilize it, but solely to profit from its value by buying low and selling higher. This restricts users to obtain the desired domain, as far too few companies offer domain name registration. This creates a monopolized market, which economically is an unfair practice and one which Butterfly strives to extinguish. Domain name registrars will frequently offer costly brokering services in domain name acquisition, which destabilize market equilibrium.

Solution

In these highly-technological times, it must come to a surprise how poorly domain names are utilized, as in that they are used solely for accessing online website pages. Butterfly aims to advance in this area much more, with a technological solution, which will liberate how Internet users interact socially and financially online.

Butterfly's vision is to establish a new era in domain name creation and ownership with the end goal being to create the future of the decentralized Internet for online users. Today websites are constantly being blocked by hostile state actors; with Butterfly your name lives on the blockchain forever and can't be taken down. The Butterfly Protocol takes control back from centralized authorities and gives it to the people who own the names. When someone acquires a domain name within the Butterfly Protocol, they own it forever.

With a blockchain-based DNS, registry operators will have flexibility and will get more opportunities when they obtain domain names. It will enable them to tailor a name to their specific niche.

Butterfly has developed a browser extension that eliminates any accessibility and censorship issues. As soon as an Internet user uses the extenstion, they will be able to access any online content they wish to engage free of censorship. This means that publishers are free to produce all kinds of content, which will likely increase their audience and bring them a bigger revenue stream. Butterfly Protocol content creators will not be restricted by censorship and their users will be able to always access quality content through the web-browsing extension.

Butterfly enables individuals to execute a single transaction and own their domain name forever, free of future payments, which are currently standard, as simple as that. Once a domain name is created and acquired, the initial registrar is its sole owner. This in itself is a major breakthrough in how domain name ownership works. Butterfly has also developed an inherent ecosystem with a native cryptocurrency token, which allows users to create, sponsor, and execute domain names and their creation – this will be covered further and in more detail in this documents.

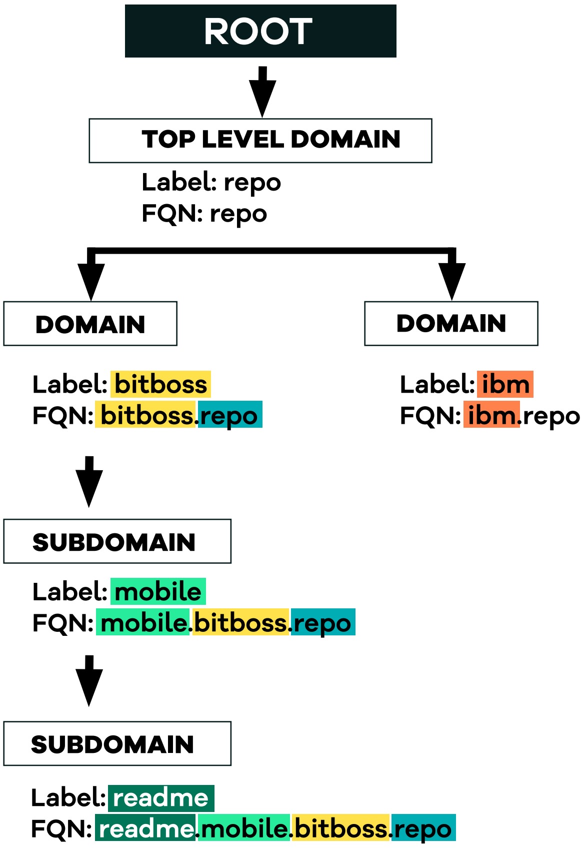
Furthermore, with Butterfly the network allows for highly-personalized domain names and extensions. As per the previous example, one would be able to acquire "companyidentity.carrentals", thus enabling them to present their own personal brand in the most accurate way. This is made possible through the Governance Smart contract which is detailed later in this paper.

Butterfly has developed an intricate ecosystem which brings immense freedom to the domain name registration industry. Any holder of the native Butterfly token will be able to sponsor new top level domain creation and initiate auctions for highly sought-after names. One a top level domain is created, all Butterfly token holders will receive a percentage of tokens specific to that domain that they can use to create subdomains with. An auction will also be started so that non-token holders can also obtain tokens for the top level domain.

Global Identification is also a major feature with Butterfly, as users acquire a Fully-Qualified Name (FQN), e.g. john.smith.id. Moreover, this FQN can be used as credential access to various social media accounts as well as to cryptocurrency wallets. The latter feature allows users to record wallet addresses in the domain, support different digital currencies, and allow transfers via easily-comprehensible FQNs instead of confusing wallet address symbol combinations.

Butterfly Naming Conventions

The following diagram illustrates the naming conventions used in this paper. The system starts with a nameless Root Domain. A top-level domain (TLD) is the beginning of a fully qualified name (FQN) in Butterfly. All TLDs are subdomains of the Root Domain, which is an invisible entity in the system. Domains can be created under the TLD, and each domain can have unlimited subdomains, which in turn can have subdomains of their own and so on. The FQN is defined as the combinations of domain labels, with the TLD label being the furthest to the right; "repo" is the TLD in the FQN "mobile.bitboss.repo".



ROOT

TOP LEVEL DOMAIN

Label: repo
FQN: repo

DOMAIN

Label: bitboss
FQN: bitboss.repo

DOMAIN

Label: ibm
FQN: ibm.repo

SUBDOMAIN

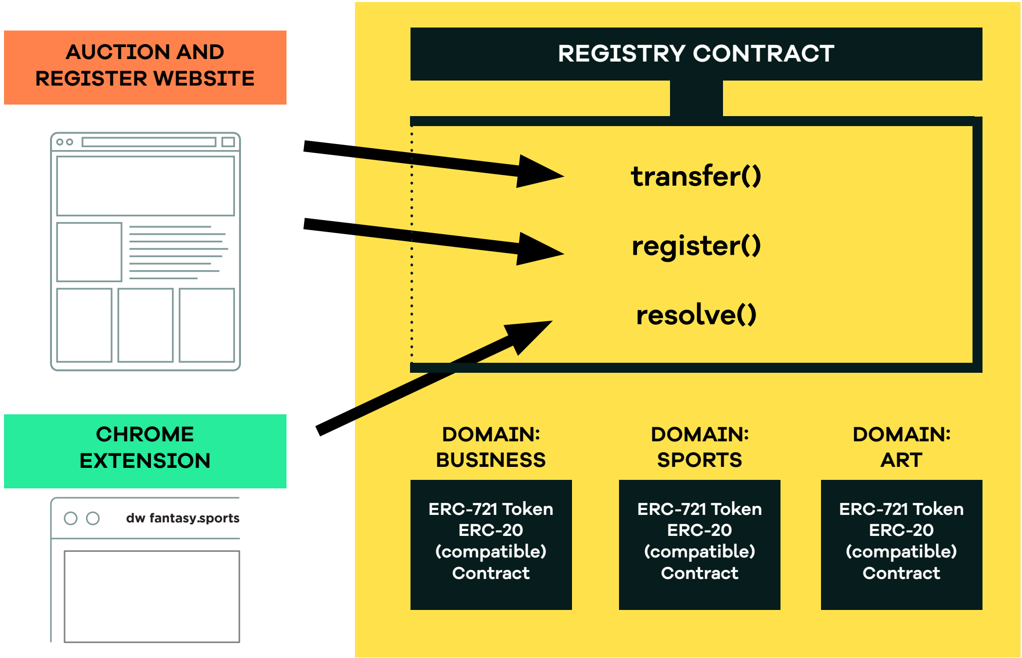
Label: mobile
FQN: mobile.bitboss.repo

SUBDOMAIN

Label: readme
FQN: readme.mobile.bitboss.repo

Architecture

The Butterfly Protocol uses Ethereum contracts and tokens to track web name ownership. The term "domain" is used to represent a single name in the system. Each domain except the root domain has a parent, and the domain hierarchy forms a name or path to retrieve that domain's resources. This is analogous to domains and subdomains in a traditional DNS system, except subdomains can continue to be created under other subdomains indefinitely. For example for a web name of players.nfl.fantasy.sports, "players" is a subdomain of "nfl", which is, in turn, a subdomain of the domain "fantasy", which is in turn a child of the top level domain "sports".


AUCTION AND REGISTER WEBSITE
CHROME EXTENSION
dw fantasy.sports
REGISTRY CONTRACT
transfer()
register()
resolve()
DOMAIN: BUSINESS
ERC-721 Token ERC-20 (compatible) Contract
DOMAIN: SPORTS
ERC-721 Token ERC-20 (compatible) Contract
DOMAIN: ART
ERC-721 Token ERC-20 (compatible) Contract

Each domain is represented by a non-fungible token in a standard ERC-721 contract called "RegistryToken". There is only ever one ERC-721 token on the public Ethereum blockchain for a specific domain. The Registry contract owns the RegistryToken contract and uses it to keep track of who the owner of a domain is. The Registry contract that contains all of the other domain information (aside from who the owner is), and it maintains the hierarchy between domains. The Registry contract creates an instance of the RegistrarToken contract for a domain (note that this is different from the RegistryToken contract). The RegistrarToken contract manages the ERC-20 compatible tokens for a domain; those tokens can be used to buy subdomains of the domain they are associated with.

Registry ERC-721 Contract

The primary values that get stored for each domain are:

- Label: the domain name (ex: "fantasy")
- Parent: the parent domain (ex: "sports")
- Token Contract: a pointer to the ERC-20 compatible contract specific to this domain
- Owner: the Ethereum public key representing the owner of this token/domain
- Record: a type and pointer used to lookup the data for the domain
- Price: the cost in Ether for each domain
- Tokens to create new: the number of ERC-20 compatible tokens that must be burned to create a subdomain

Registry Contract Functions:

register: Creates an ERC-721 token and sets the domain fields to configure it. The Register function in the smart contract will be called from the Registrar website when a user registers a new domain. The Registry contract checks that the owner has enough of the ERC-20 compatible 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 domain 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.

RegistrarToken ERC-20 Compatible Contract

A set of ERC-20 compatible tokens can be created for each new domain using the RegistrarToken contract. The ERC-20 compatible tokens are then used to establish value within that domain. This means that owners of the ERC-20 compatible tokens may have the ability to create a subdomain by burning some amount of their tokens if the parent has that functionality enabled.

The system starts with a root domain that is owned by the Butterfly Protocol itself. Top level domains (TLD) are created from there by burning root ERC-20 compatible tokens. The ERC-20 compatible tokens for the TLD are then auctioned off to anyone that wants the ability to create subdomains under the TLD. 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 domain's ERC-20 compatible tokens can create subdomains even though the parent domain has a single owner. This parent/child relationship continues downward indefinitely. For example, a subdomain called "company1" could be created under the parent domain "software" which in turn has a parent TLD "business", representing a fully qualified name of "company1.software.business", which could be used in the Butterfly browser extension and other supported clients to reach the "company1" website.

Each domain points to a data store to hold information about that domain. Initially, the most common type of data will be ipv4 and ipv6 values for the domain, to point at the website for that domain. These IP address values may never be updated after domain 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 domain; 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.

Governance Contract

The Governance contract owns the root domain and all TLDs and is therefore responsible for creating TLDs and managing the sponsorship of each TLD. This contracts kick off the auction process and handle the distribution of the associated ERC-20 compatible tokens.

Note that the Governance contract will allow BitBoss to create and own 5 TLDs for promotional purposes. For example, BitBoss will own the .human TLD to use within its mobile app to give away .human subdomains.

A BUTTERFLY TOKEN holder must burn 10,000 tokens to sponsor a new TLD name. This amount goes down by 10 tokens daily, which is a mechanism intended to incentivize continued sponsorships of new TLDs. The Governance contract manages the current cost to sponsor a TLD, and it burns the tokens that are spent by a BUTTERFLY TOKEN holder for sponsorship.

Checkpoints are used to determine how many BUTTERFLY TOKENS each account owns prior to the start of a new TLD auction. This allows the Governance contract to precisely distribute ERC-20 compatible tokens for the TLD at the end of the auction across all BUTTERFLY TOKENS holders.

Governance Contract Functions:

The following functions are used by the auction website and clients to operate and participate in auctions, as well as facilitating creation/ sponsorship of a new TLD.

auctions: Returns information about each auction, including:

- State (available or sponsored)
- Label (TLD name)
- Index
- Start date
- Address of associated Token contract
- Sponsor
- Checkpoint used
- Total amount raised

totalAuctions: returns the total number of auctions

auctionsByIndex: retrieves an auction

sponsorshipCost: returns cost to sponsor a TLD

sponsor: sponsors a TLD

currentTranche: a view that returns what tranche an auction is currently on. A tranche is a period of time, for example, a typical auction will have 10 tranches, each one last 24 hours.

bid: payable function to bid on an auction

raised: a view that returns the amount raised for the auction

raisedByTranche: a view that returned the amount raised for a specific tranche of an auction

bidFor: returns the total sum of bids that an account has made for an auction

payoutByTrancheFor: total payout for an account for a specific tranche

payoutFor: total payout for an account

airdropRewardFor: uses a checkpoint to calculate how much of the total airdrop goes to a specific account

claim: mints ERC-20 compatible tokens for:

- sponsor reward (if the specified account was the sponsor)
- airdrop reward (if the specified account holds BUTTERFLY TOKENS)
- auction payout, based on the total ETH contributed by the specified account

claimed: returns a boolean as to if the tokens have already been claimed for an account

GovernanceToken ERC-20 Compatible Contract

This is the contract that tracks the number of BUTTERFLY TOKENS that each account has. It is used by the Governance Contract to create checkpoints and distribute a TLD's ERC-20 compatible tokens at the end of an auction.

GovernanceToken Contract Functions:

balanceAt: retrieves the balance of BUTTERFLY TOKENS for an account, for a checkpoint

currentCheckpoint: gets the current checkpoint information

createCheckpoint: creates a new checkpoint

Butterfly Clients

Multiple clients will be created for easy access into Butterfly:

Browser extension: Allows users to browse using the new domain 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 Butterfly and therefore will 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 Butterfly 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.

Butterfly Use Cases

Now that we know how Butterfly ecosystem will operate, let's delve into how it can be applied in real-world scenarios. These use cases will also showcase the scope of Butterfly protocol structure but also display the towering layers of features that it encompasses.

Censorship

In instances of a website being continually blocked by a hostile state actor, the users have to continually keep track of the new website URLs to maintain access to the given site. The online company purchases the domain with the FQN "xyz.info" from a Butterfly auction and now owns it permanently. Their users can now consistently access the blocked website using the Butterfly browser extension by typing in the same value "xyz.info" every time. Consequently, Butterfly protocol eradicates any governmental censorship that has been administered thus far, and enables Butterfly participants to reap the benefits of decentralization and censorship-proof ecosystem.

Proof-of-freedom

Freedom of expression is Butterfly's forte and is one of the main reasons for its disruptive nature. A mobile application will be created to enable people to easily acquire a ".human" subdomain name and then use that domain as to create content for others to read. No person or organization can block your content, censor you, or cancel your account. You are the sole owner of everything that you create and possess. This will be the use case that we launch the platform with. It serves as a showcase for how the Butterfly platform can be used to benefit society.

Global identification

Let's say that a user obtains a Butterfly domain with a fully qualified name of "john.smith.id". This FQN becomes their global identify and can be used through the Butterfly 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 domain for different cryptocurrencies allowing digital assets to be sent to a human-readable FQN instead of an incoherent address. Rendering FQN as a global identity means that Butterfly users will be able to complete all of the aforementioned actions in a completely decentralized manner. Besides, the global identification is exclusively maintained and employed by the owner whose identification and personal data stay beyond the reach of any authority.

Token generation event

A subdomain can be acquired underneath a parent domain. This subdomain can be locked to prevent new subdomains from being created underneath it. The owner can then run their own fundraising campaign (ICO, IEO, STO, etc) with the supply of ERC-20 compatible tokens assigned to that domain. These tokens can be generated for any domain with no coding or contracts needed. The token is directly associated with a domain in Butterfly, so it is easily searchable and usable by domain 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 domain "tradingcard.sports" and therefore has all the utility tokens for that domain. Those tokens can be sold to game players to create a subdomain 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 subdomain 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.

Github

The recent purchase of Github by Microsoft has revealed yet another excellent use case of Butterfly. The platform 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 TLDs and subdomains are becoming easy to understand. We intend to release ".repo" as one of the first TLDs and quickly integrate a Git implementation. If only a small fraction of the 57 million repositories run on Butterfly, the ".repo" TLD will be extremely valuable.

Fractional Ownership Type 1

Antiques can be well represented by non-fungible ERC-721 tokens. A Butterfly subdomain under the "antiques" TLD, for example, can be created for every physical antique item with the associated 721 token. The subdomain name could be a serial number of the antique item or a unique description of it. The antique owner can sell off fractional ownership by generating ERC-20 compatible tokens for the antique item. Each person interested in owning a portion of the antique item can purchase specific number of the associated ERC-20 compatible tokens. The fractional owners anticipate the physical item's value increment over time and they can sell or trade their tokens to other parties. The owner of the antique item can sell it, at which time they prove their ownership with the ERC-721 token and transfer that token to the new owner.

Fractional Ownership Type 2

A bar of gold can be registered by its serial number as a non-fungible ERC-721 token within Butterfly. Each bar would be created as a name under the "gold" TLD, for example "A444581.gold". Assume that the bar is 1 kilogram - then 1000 ERC-20 compatible tokens would get created, each token representing 1 gram of gold associated to that specific physical bar. The ERC-721 token would be owned by the entity that has physical possession of the gold, and the ERC-20 compatible tokens would be distributed and owned by the various fractional owners. The ERC-20 compatible tokens could be sold and traded on a decentralized website created to specifically target gold exchanges, and a fractional owner could also simply send their gold to another user using an Ethereum wallet such as MetaMask.

Butterfly Tokenomics

The native digital cryptographically-secured protocol token of the Butterfly protocol is a major component of its ecosystem, and is designed to be used solely within the network. The IEO process starts with the circulation of 100,000,000 BUTTERFLY TOKENS which have three main purposes to start with:

- Token owners can sponsor the creation of new TLDs
- Token owners receive an air drop of 15% of all ERC-20 compatible tokens for every TLD created

Once the BUTTERFLY TOKENS are distributed, the Governance smart contracts take over. This smart contract will own the root domain and will facilitate the creation of all future TLDs.

Since the registrar is run as a DAO we need a mechanism to suggest new TLD names and to create them. This is where the BUTTERFLY TOKEN comes into play.

Sponsorship

A BUTTERFLY TOKEN holder can spend their tokens to sponsor the creation of new TLDs. They can choose any available name that they want, or refer to the most popular TLD names that others would like to see created. When a new TLD name is sponsored, the TLD gets automatically created and a 10 day auction starts for the sale of its associated ERC-20 compatible tokens.

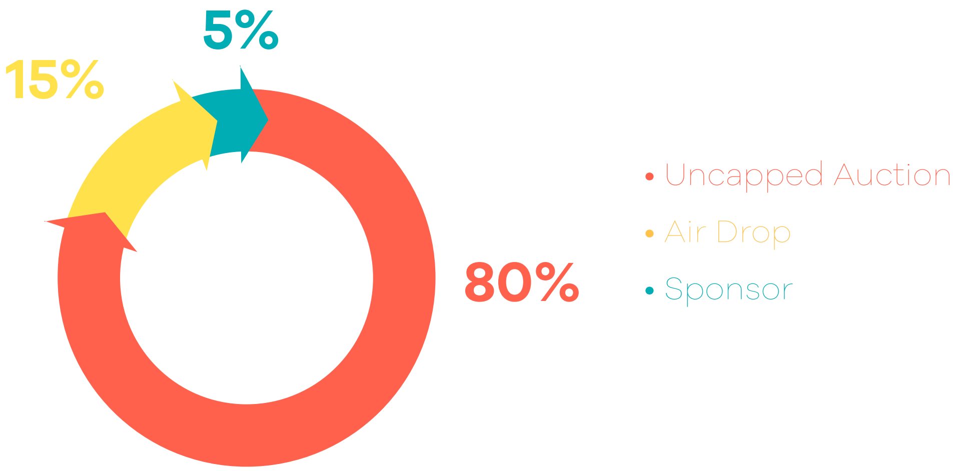
The initial cost to sponsor a TLD is 10,000 BUTTERFLY TOKENS. This cost goes down by 10 tokens every day, starting from the day that the Butterfly DAO is launched. These cost reductions are done to ensure that it costs more to sponsor high value TLD names, which will be the ones created early on. Also this approach ensures that the system continues to generate interest with medium to lower value TLD name as time goes by.

The sponsorship functionality provides ways for the BUTTERFLY TOKEN holders to have a stake in the governance of the registrar.

Let's assume that ".sports" is the TLD that has the most potential and someone therefore decides to sponsor its creation. That token holder spends the required amount of BUTTERFLY TOKENS by sending them to the Governance contract. Those tokens are burned at that point, meaning they can never be used again by anyone (thereby raising the value of the remaining tokens in circulation).

The Governance contract controls the process of auctioning off a subset of the ERC-20 compatible tokens for the ".sports" TLD, and it will start an uncapped auction. Bidders spend ETH and are rewarded based on the ETH that they contributed as a percentage of the total ETH contributed.

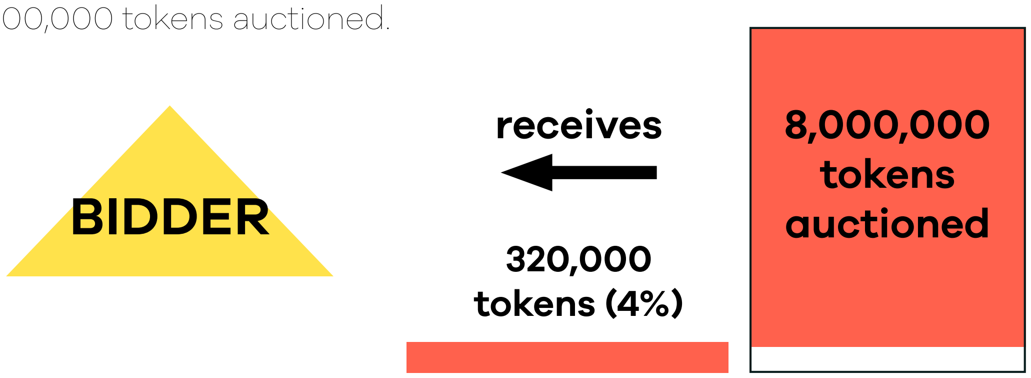
By way of example, the Governance contract will create a supply of 10,000,000 ERC-20 compatible tokens for ".sports". It will allocate:



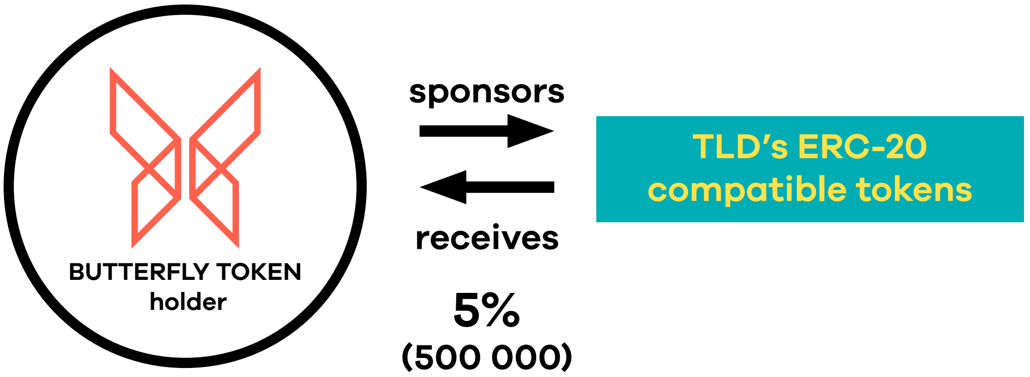
Over the course of the 10 days, bidders send ETH to the Auction smart contract. At the end of the 10 days, each bidder's contributed amount is divided by the total ETH collected. In this case, assume our bidder contributed 20 ETH out of a total of 500 ETH contributed by all bidders. Our bidder would now receive 4% of the ERC-20 compatible tokens that were auctioned (20/500 = 4%). The formula for this is:

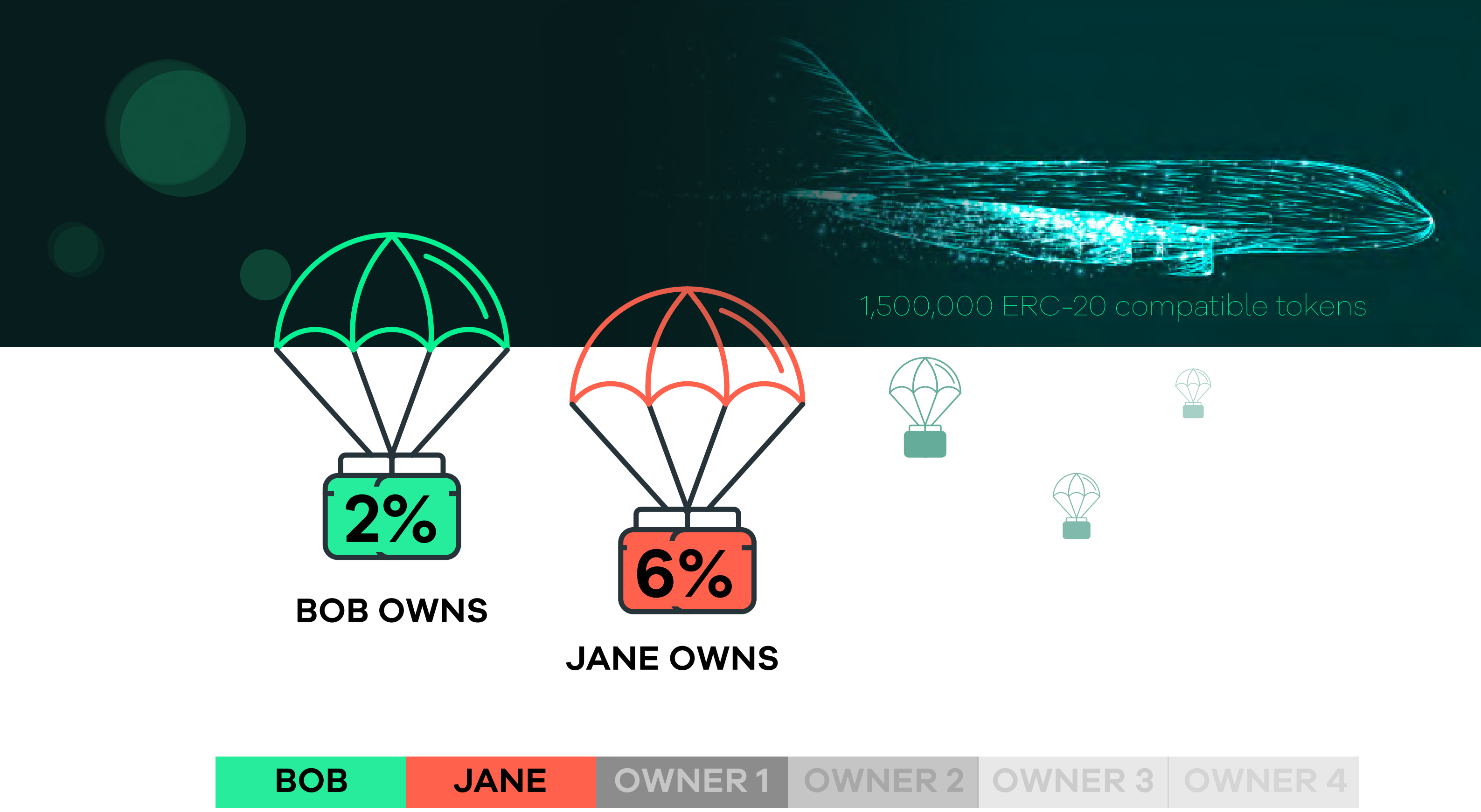
$$\frac{\textbf{ETH}\ \text{contributed by Bidder}}{\textbf{Total ETH}\ \text{contributed}} = \textbf{\% Tokens}\ \text{Received by a Bidder}$$

In this example, the bidder receives 320,000 tokens, which is 4% of the 8,000,000 tokens auctioned.



The BUTTERFLY TOKEN holder that sponsored the TLD name creation receives 5% of the TLD's ERC-20 compatible tokens, which would be 500,000.

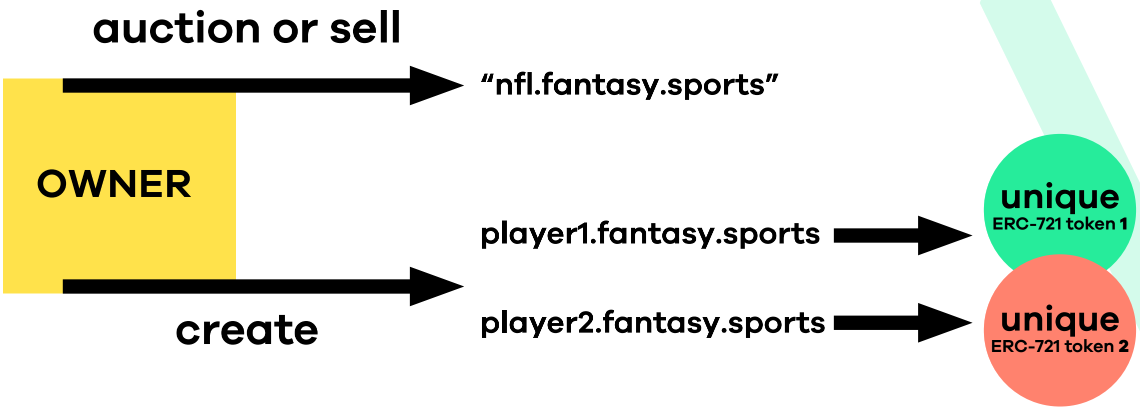




1,500,000 ERC-20 compatible tokens (15%) are air dropped proportionally to all owners of the BUTTERFLY TOKEN. By way of explanation, Bob owns 2% of the total BUTTERFLY TOKENS in circulation, and Jane owns 6%. Bob therefore receives 30,000 of the ".sports" ERC-20 compatible tokens and Jane receives 90,000.

After the auction closes the new owners of the ERC-20 compatible tokens will now be able to acquire subdomains by burning a predetermined number of those ERC-20 compatible tokens for each subdomain. The first person to register a subdomain acquires it. The smart contract will specify a higher burn amount in the first week to prevent people from "domain parking" high value subdomains. This amount will reduce day by day to encourage the creation of lesser value subdomains. By example, a token owner must burn 1000 tokens to register "fantasy" under the "sports" TLD. The "fantasy" subdomain is now irrevocably associated with a specific non-fungible ERC-721 token that is owned by the person who registered it. People using Butterfly will land at the owner's website and other resources when navigating to "fantasy.sports".

The owner can now create their own supply of ERC-20 compatible tokens associated with the ".fantasy" subdomain. The owner can then start their own economy around the "fantasy.sports" name. They could simply point the TLD to an IP address or they could creatively use the ERC-20 compatible tokens.



Since these ERC-20 compatible tokens are fungible utility tokens they can have many potential use cases for the owner's economy. For example the owner can auction or sell subdomains such as "nfl.fantasy.sports". Or they could create subdomains player1.fantasy.sports and player2.fantasy.sports, where each player is represented by a unique ERC-721 token with its own supply of ERC-20 compatible tokens. Very creative new business models for fantasy sports can therefore be created.

Buy Now Feature

In addition to the uncapped auction functionality the subdomain owners can sell a domain that they own using the Buy Now feature. This feature lets an owner list that domain name for sale at a specific price in Ether.

The seller receives the proceeds directly into their wallet. The ERC-721 token is transferred to the buyer as a result of the transaction.

Note that when selling a non-fungible 721 domain token (let's use fantasy. sports as the example), all ERC-20 compatible tokens for that domain that have already been sold or transferred to other people cannot be revoked. The entire model breaks if the 721 owner could pull back ERC-20s. People have already used those fantasy.sports ERC-20s to acquire subdomains, for example soccer.fantasy.sports. They have therefore also created ERC-20s for those sub-subdomains. You can't take ownership away from other people that have already started new economies.

The value of a domain being sold is determined by:

- The perceived value of the domain name
- How many ERC-20s remain with the ERC-721 token that get transferred to the new owner
- What subdomains have already been created off of the domain by other people

Auctioning a Domain (ERC-721 ownership)

A "reverse clock" auction contract and website will be created to facilitate a domain owner selling their domain. Note that this is separate from the auction process that we will use to initially sell TLDs.

The ERC-721 domain 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 TLD begins. The price (in Ether) of the TLD 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 TLD 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 compatible tokens linked to that domain. The ERC-721 owner can trade, sell, or auction the token at any time transferring ownership of that domain.

Raised funds allocation

Butterfly will use a portion of the funds raised to invest back into the platform for marketing and development efforts.

This includes development of add-on services on top of the Butterfly platform, including:

- client applications that allow users to browse to Butterfly domains including browser extensions, a Butterfly specific browser, a DNS Gateway, search engines
- a mobile app for publishing and viewing decentralized content (this is the Butterfly app, which we can show a prototype of during the IEO sale)
- enhancing our auction website

Token burn

10,000 Butterfly tokens get burned to sponsor a new TLD. That amount goes down daily based on how many other TLDs that have been sponsored. By burning tokens during the sponsor process, the overall value of the Butterfly token should increase over time.

Team and accomplishments

Matthew Dickson, CEO and Co-Founder

Matthew started his career practicing law in New York City. He represented clients in the insurance and finance sectors before forming a diversified financial service company. After the sale of the given company, Matthew shifted his focus and formed a private equity firm specializing in early-stage investments. With a focus on the real money gaming sector he made investments in casinos, online content providers and manufacturers.

Missing the joy of running his own company, Matthew founded Poydras Gaming Finance Corporation, which he took public on the Toronto Venture Exchange in 2014. Poydras, which was recently sold to the Las Vegas-based gaming company AGS, owned 2,600 slot machines. The machines were leased to Indian tribes in the United States.

During his time at Poydras he started an emerging technology lab. Once again following his passion for early-stage startups Matthew spun BitBoss Corporation out of Poydras and assembled a highly talented team of blockchain developers to pursue opportunities in the gaming sector. Since founding BitBoss he's been issued a patent for provably fair gaming and has numerous pending patent applications for blockchain gaming solutions.

BitBoss solutions now include a gaming platform, lottery solution and an ecosystem running on the Bitcoin blockchain. BitBoss will soon release their first hardware device that aims to change how casino gamblers use and store casino credits.

Matthew's legal background has allowed him to understand the regulatory environment and he was asked to be on the Gaming Standards

Association blockchain workgroup. He has also worked with testing labs to help write testing standards that allow for the inclusion of blockchain technologies.

Alex Shore, CTO and Co-Founder

Alex has been developing enterprise software for 25 years and has been the founder of 3 software startups. He has extensive management experience in both small and large companies including the use of scaled agile methodologies to empower multiple scrum teams to deliver high-quality software in a predictable fashion. Alex has worked across many domains and has significant experience in the travel/hospitality industry as well as the gaming industry.

Alex has a background in architecting and deploying highly scalable integration platforms and working closely with vendors and partners to seamlessly connect with their systems. He is currently developing blockchain applications and managing a team of cryptography and blockchain experts including several offshore development teams. His technical expertise includes C#, Javascript, C++, REST web services, Azure Cloud Services, Angular, Ionic, and Node.js. Alex has a mobile device background that extends all the way back to creating applications on the first Palm Pilot PDA devices. He holds a patent for early support of timezones on mobile devices.

Justin Laue, Chief Engineer and Co-Founder

Justin has over 25 years of software development and architecture experience. He has a background in low-level programming for the cable and video on demand industries, where he developed his Linux expertise and leveraged his deep knowledge of C++ and Java. He was the engineer primarily responsible for having his company receive an Emmy award for video on-demand solutions. Justin has managed numerous international development teams over his career.

In recent years, Justin has become a blockchain expert, creating solutions on both private and public blockchains and contributing to large, high visibility software projects including Bitcoin Unlimited and Tokenized. Justin is the creator of a Bitcoin blockchain explorer Bitfire.io. He creates APIs in Node.js that interact with public blockchains and has created client-side javascript libraries that interact with multichain and Bitcoin. Justin has expertise with MongoDB, Angular, Ionic, and Reactive programming.

Josh Robinson, Chief Architect and Co-Founder

Josh is a code craftsman, cryptographer, and technologist. He is a 19-year software veteran who thrives on creating and experimenting with cutting edge technologies.

Josh served as an architect and lead engineer for large corporations such as Aetna, Bloomberg, and Red Cross. He created the Ruby gem "countries" which have had over 13M downloads, and he authored a book on Meteor.js ("Introducing Meteor").

Josh changed his focus to founding startups where he could fully leverage his complex skillset of javascript frameworks, highly scalable database platforms, cryptography, and web & mobile development. He was the co-founder at YouBase where he utilized advanced cryptography techniques to empower an individual-centric data exchange. He then co-founded BitBoss where he's spent the last 5 years as a blockchain expert, focusing on innovative decentralized platforms that power a DNS replacement and gaming solutions.

Josh created the open-source Keyring libraries (https://github.com/BitbossIO/keyring) that facilitate faster and easier Bitcoin blockchain development. He's been issued a patent for provably fair gaming.

Cort Langworthy, CCO and Co-Founder

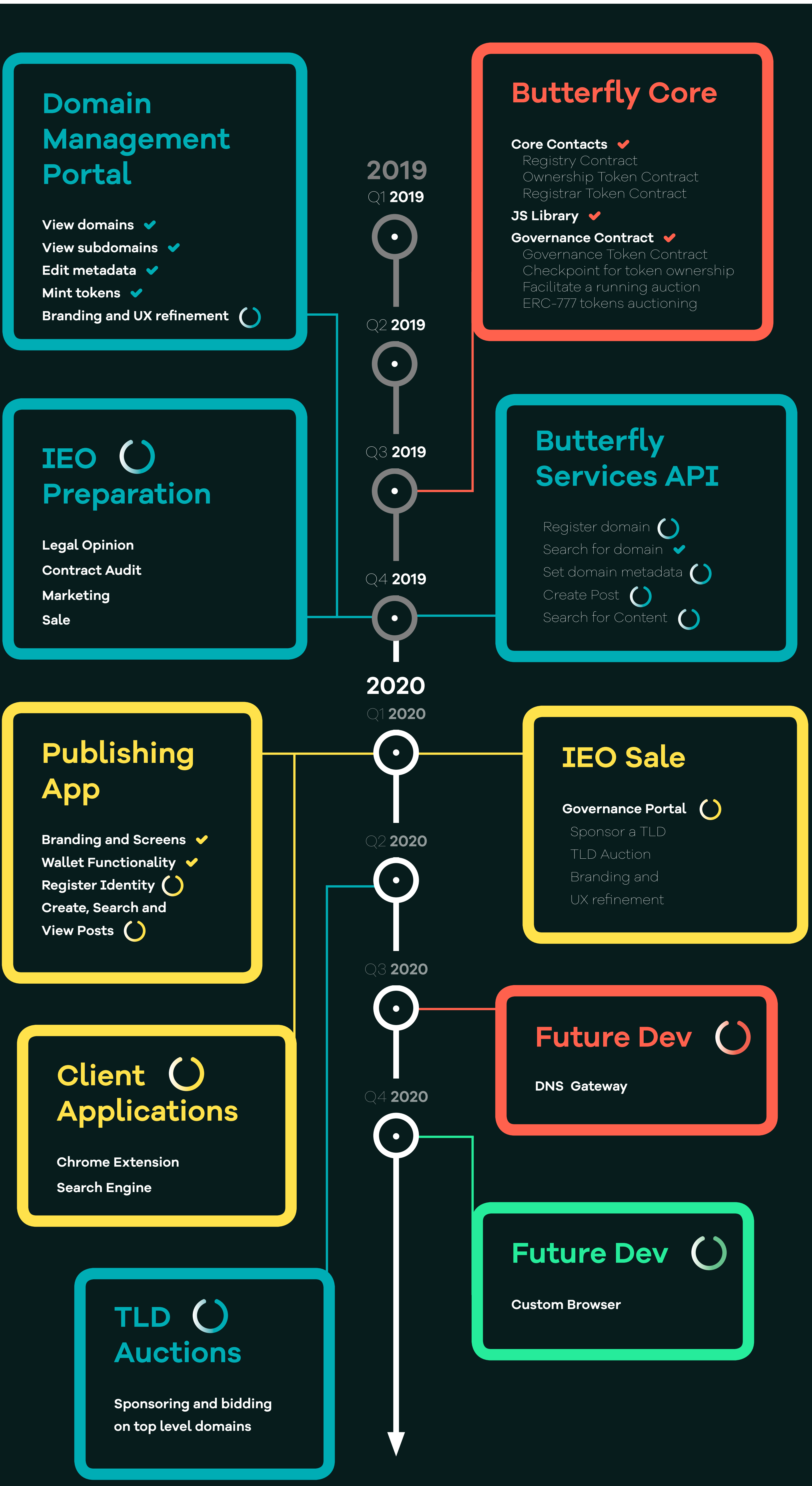
Cort is an award-winning creative with the skills to ideate, design, and develop user-focused digital projects as well as manage the teams that bring them to life. He approaches all projects with a strategic UX mindset, taking into account the overall business goals, brand voice and user behavior that will drive the most effective solutions.

Before joining BitBoss, Cort has served as both a Director and VP for numerous marketing agencies. He drove business development at Big Theory to the point where it was named to Inc. 500 and acquired by Xceed, Inc. Cort has recently served as a UX lead on data visualization tools for Google. As the chief creative officer at Bitboss, Cort focuses on user interfaces and the branding of BitBoss' unique product set. He also manages the tactical marketing teams.

Roman Tiutiunnyk, Development Project Manager

Roman is the project manager of the BitBoss offshore development team. He handles all recruiting and day-to-day management for our larger projects that include Angular and React Native mobile development, custom Java plugins for our Android applications, as well as the creation of web services and backend solutions using Java and Node.js. Roman is heavily focused on immaculate design and high-quality code.

ROADMAP



Domain Management Portal

- View domains ✓
- View subdomains ✓
- Edit metadata ✓
- Mint tokens ✓
- Branding and UX refinement ○

Butterfly Core

Core Contacts ✓
- Registry Contract
- Ownership Token Contract
- Registrar Token Contract

JS Library ✓

Governance Contract ✓
- Governance Token Contract
- Checkpoint for token ownership
- Facilitate a running auction
- ERC-777 tokens auctioning

2019

Q1 2019

Q2 2019

Q3 2019

Q4 2019

IEO ○ Preparation

- Legal Opinion
- Contract Audit
- Marketing
- Sale

Butterfly Services API

- Register domain ○
- Search for domain ✓
- Set domain metadata ○
- Create Post ○
- Search for Content ○

2020

Q1 2020

Publishing App

- Branding and Screens ✓
- Wallet Functionality ✓
- Register Identity ○
- Create, Search and View Posts ○

IEO Sale

Governance Portal ○
- Sponsor a TLD
- TLD Auction
- Branding and UX refinement

Q2 2020

Q3 2020

Client ○ Applications

- Chrome Extension
- Search Engine

Future Dev ○

DNS Gateway

Q4 2020

Future Dev ○

Custom Browser

TLD ○ Auctions

Sponsoring and bidding on top level domains

BUTTERFLY
PROTOCOL

Glossary of terms

Butterfly - A 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 that is directly under the root domain. For example "sports" can be a TLD and "fantasy.sports" represents a subdomain of "fantasy" under the top level "sports" domain

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

Domain - A name of some entity within Butterfly. There can be many subdomains under a parent domain. A subdomain is similar to a subdomain in the current domain name system

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

IPFS - InterPlanetary File System (ipfs.io)

ERC-20 - Butterfly uses ERC-20 compatible tokens as fungible tokens that are used (burned) to create subdomains for the domain that they belong to. Any reference to "ERC-20" in this document means that the token is ERC-20 compatible; it may contain additional features beyond the base ERC-20 definition

IEO - initial exchange offering, a way to purchase BUTTERFLY TOKENS

BUTTERFLY TOKEN - the token acquired during the initial exchange offering. Owners of this token get to sponsor the TLDs creation and they receive ERC-20 compatible tokens for each TLD created.

butterflyprotocol.io