COTW: Ushering in the Next Wave of Crypto Adoption with Blockchain Domains

Fusing payments, Web3, and decentralized identity, blockchain domains are proving to be critical infrastructure capable of ushering in the next wave of crypto adoption. We review traditional internet and blockchain domain systems, how blockchain domains work from a technical perspective, spotlight key providers, and ponder the future benefits of blockchain domains in this week's Chart of the Week.

The Downsides of DNS: When surfing the internet, a user will enter a URL into their browser to see a webpage. To aid operability and avoid collisions, however, internet connected devices communicate with each other using unique numeric identifiers called Internet Protocol (IP) addresses. As such, the Domain Name System (DNS) was created in 1983 to act as a directory of domain names and IP addresses, linking human-readable addresses to computer-readable IP addresses, working similarly to a phone book. As an example, entering www.gsr.io into a web browser will query a DNS server to request the domain's IP address, in this case 178.79.182.244, after which the browser will make an HTTP request to the server hosting the IP address to return the webpage for rendering in the browser. While DNS is a public registry, it is governed by the Internet Corporation for Assigned Names and Numbers (ICANN), which also oversees domain registrars such as GoDaddy.com. DNS is a foundational pillar of the traditional web, ensuring that each domain resolves to a single IP address and improving the web browsing experience with human-readable names. The centralized architecture of DNS, however, results in several misgivings. First, there is high censorship potential, for example, by a controlling regime censoring an opposition website simply by targeting DNS. Second, privacy breaches are made much easier, given the ability to monitor online activity simply by monitoring DNS requests. And finally, there are abundant security concerns due to the introduction of additional attack vectors such as with Denial of Service or DNS Spoofing attacks. And despite the Hypertext Transfer Protocol anticipating future functionality such as digital payments when it was created (see the "reserved for future use" 402 Payment Required HTTP status code), innovation around DNS has been slow to other facets of the internet and technology more broadly.

Blockchain Domains: Blockchain domain name systems are suites of smart contracts on public blockchains functioning as distributed, open, and extensible naming systems. Like their DNS counterparts, blockchain domain systems map human-readable names like 'alice.eth' or 'trade.crypto' to machine-readable identifiers, such as blockchain addresses, content hashes, and metadata. However, unlike traditional domain names that are controlled by centralized entities, blockchain domain names, represented as NFTs, are custodied by their owner, with a separate public registry in the form of a smart contract. Such decentralized architecture makes blockchain domains censorship resistant, transparent, and more open and secure than traditional domain names. Moreover, blockchain domains offer greater functionality, given their programmable, composable nature. This is ushering in an improved user experience by allowing users to send and receive funds using their domain name, replacing sandboxed app-specific usernames via a single sign-on, giving users control over their data, simplifying web3 creation, development, and adoption, and playing a critical security role by adding decentralized domain names to decentralized websites and file storage. As "alternative roots", blockchain domains are not part of the current DNS, requiring a plugin or web3 platform like Opera or Brave to work, but the space is evolving quickly.

Blockchain Naming Systems Work: We provide an example of how Ethereum Name Service (ENS) works, though note that other blockchain naming systems such as Unstoppable Domains work in much the same way. In addition to functioning as an Ethereum-based naming system mapping text-based names to non-intuitive identifiers such as crypto addresses and content hashes, ENS also supports reverse resolution, making it possible to associate metadata such as canonical names (the host name of a computer or network server) or interface descriptions with Ethereum addresses. To do so, ENS uses a system of dot-separated hierarchical domains and owner-controlled subdomains, such as alice.eth (a domain name) and iam.alice.eth and friendof.alice.eth (subdomains, for example, for Alice and her friend). Smart contracts called registrars own top level domains, and anyone may obtain ownership of a domain by following the registrar contracts' rules. Note too that ENS supports DNS names for use on ENS, allowing owners to add blockchain based functionality to their traditional web domain name. Architecturally, ENS has two components, the registry and resolvers. The registry is the core contract of ENS, maintaining a mapping of all domains and subdomains to their owner, resolver, and time-to-live. Here, owners may be a user (externally owned account) or a smart contract, while a registrar is the smart contract responsible for allocating subdomains. Resolvers, on the other hand, are responsible for the actual process of translating names into addresses and other data. Importantly, the method a resolver implements to retrieve a record depends on the type of record being queried, meaning that when a domain is entered into a browser, the resolver returns the IPFS hash and when being used to send ETH, the resolver returns an Ethereum address, and so forth. Resolving a name in ENS involves putting the two components together - asking the registry what resolver is responsible for the name, followed by asking the resolver to answer the query. Importantly, this two-component design allows record types to be included in a resolver and for new functionality to be added by simply releasing a new resolver, avoiding centralized upgrade mechanisms and the complexity of putting every possible record type into the central registry. Lastly, note that ENS uses a process called Namehash to turn ENS names into fixed-length 256-bit cryptographic hashes to increase efficiency and preserve hierarchical properties.

- **Example:** If a user wanted to send ETH to GSR, he or she would enter gsrmarkets.eth into their wallet to field, which would then ask the ENS registry which resolver is responsible for gsrmarkets.eth. The registry would then return the smart contract named ENS: Public Resolver 2. Next, the wallet will then query this resolver for the address of gsrmarkets.eth to receive 0xAa0542346Dc0fbB27D60283463F00D7bA4644B1A. This process is abstracted away from the user and allows for the transaction to occur without needing to enter the 42 hexadecimal character address, improving UE and avoiding accidental loss.

Key Players: There are several players offering blockchain domain naming services, such as:

- **Namecoin:** Launched in 2011 and offering the .bit extension, Namecoin was one of the earliest attempts to use blockchain technology for decentralized naming with its system for registering domain names on Bitcoin. While novel and innovative, Bitcoin's constrained coding functionality limited significant adoption.

- **Ethereum Name Service:** Originating as part of the Ethereum Foundation in 2017 and created by Nick Johnson, Ethereum Name Service spun off as a separate organization in 2018 to provide decentralized naming for wallets, websites, and more. ENS has registered over 545,000 names, and is the most connected blockchain naming standard with 342 integrations. ENS views itself as a web3 public good, which guides many of its decisions. For example, ENS allows companies to register their DNS in ENS to gain ENS functionality, further promoting ENS's mission as a naming system (rather than maximizing profits). Additionally, ENS charges both registration and renewal fees with more scarce (ie. shorter) names commanding higher prices to prevent scalpers / promote legitimate use as well as ensure future name availability should an owner lose access (click here to see recently-available ENS domains). ENS recently launched its ENS governance token via a highly equitable airdrop as part of its transition to a DAO.

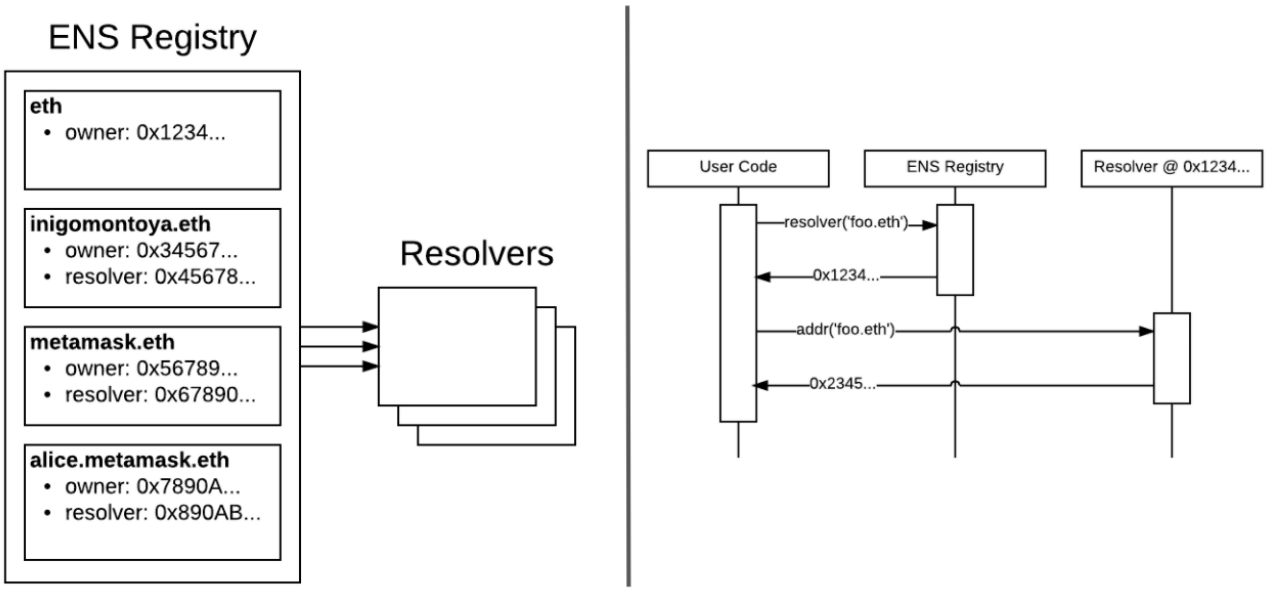
- **Unstoppable Domains:** Founded in 2018, Unstoppable Domains is a blockchain naming service with over 1.7m registered domains, including the .crypto, .zil, and .x extensions. Unstoppable domains can be used as payment addresses for wallets for over 275 tokens, as a website URL, and as a single sign-on across web3 apps, the last of which allows developers to learn more about their users and users to control what data is shared. Once purchased, Unstoppable domains are owned for life, so there are no renewal fees. Architecturally, Unstoppable Domains has a Unstoppable Name Service (UNS) and a Crypto Name Service (CNS), with the former having a simplified architecture optimized for higher transaction volumes and multiple top level domains and the latter utilizing architecture similar to that of ENS with registry and resolver components and a Namehashing process. Major browsers such as Chrome, Firefox, and Edge can be easily configured to resolve Unstoppable domains, and Unstoppable Domains is on Polygon as its layer two scaling solution.

- **Others:** There are various other decentralized naming systems, including: the Solana Name Service, which is spearheaded by Bonfida and simplifies transferring funds, developing projects, and more with its .sol domains; Decentraweb, which allows anyone to permissionlessly create and own top level domains on the Ethereum blockchain; and, Handshake, a decentralized, permissionless naming protocol where every peer is validating

and managing the root DNS naming zone to create an alternative to existing Certificate Authorities and naming systems.

Improving on Web2 with Blockchain Domains: Blockchain domain names already make sending and receiving cryptocurrency easier, add key web3 functionality with readable, decentralized domains, and allow apps to be accessed via a single sign-on. In the future it's possible, perhaps likely, that the vast majority of crypto payments are sent and received using blockchain domains, lowering loss and improving user experience. Moreover, blockchain domain-based single sign-on may serve as the foundation of digital identity, allowing users to amalgamate social media accounts into one unified universal profile, purchase items from Amazon.com without ever needing to enter log-in or payment details, and control and profit off of their own data. Additionally, it's possible DNS adopts the blockchain-based back end architecture to increase functionality, or DNS name registration within ENS becomes widespread. Such a move would bring about endless possibilities, such as enabling a traditional website to accept direct payments sent to its domain name, eliminating the need for a payments intermediary. While some of these changes could come about quickly, for example if a large web2 company enabled such functionality, we believe it will take many years of steady progress to realize the many benefits of blockchain domains, and that its exact future will be determined just as much by what happens in the DNS space as in web3. That said, blockchain domain naming systems are on their way to potentially becoming the naming system for every digital resource in the world, working with and improving upon DNS to make the web more open and decentralized and unlocking the true potential of web3 for all.

Exhibit 1: Ethereum Name Service Architecture



Source: Ethereum Name Service, GSR

Author: Brian Rudick, Senior Strategist

Sources:

Unstoppable Domains: Documentation
Unstoppable Domains: Blog
Ethereum Name Service: Documentation
Ethereum Name Service: Medium Page
The Defiant Podcast: Nick Johnson of ENS
Crypto Native: Nick.eth on .eth Twitter Names and the Future of ENS Domains
RSK Blog: Blockchain Domain Name System - Decentralizing The Web
Cloudflare.com: Learning Center

About GSR

GSR is a crypto market maker and ecosystem partner.

Founded in 2013, we specialize in providing liquidity, risk management strategies and structured products to sophisticated global investors in the digital assets industry.

We have a culture of approaching complex problems with tenacity and imagination. We build long-term relationships by offering exceptional service, expertise and trading capabilities tailored to the specific needs of our clients.

GSR works with token issuers, traders, investors, funds, miners, and cryptocurrency exchanges around the world. GSR is an investor in more than 100 projects building the future of finance and technology. We form lasting partnerships with our portfolio companies through our suite of services and global team of over 190 cryptofinance professionals.

Find out more about GSR here, or contact us at markets@gsr.io.