日本総研
The Japan Research Institute, Limited

ブロックチェーンを用いた名前解決
～分散型ネームサービスの概要～

株式会社日本総合研究所 先端技術ラボ

2024年3月21日

本レポートに関するお問い合わせ 先端技術ラボ 會田 拓海（aita.takumi.m2@jri.co.jp）

はじめに

ブロックチェーンやこれを基盤とするWeb3では、ブロックチェーンのアドレスでユーザを識別し、データを相互にやり取りする。しかし、このアドレスの可読性が低いことや、現在のTLD*1管理の中央集権性に対する課題感から、ブロックチェーンでドメイン名を管理する「分散型ネームサービス」が構想された。

分散型ネームサービスとは、ブロックチェーンを用いてIPアドレスやブロックチェーンのアドレスなどとの名前解決を提供するサービス。IPアドレスの解決を提供するサービスもあるが、従来のDNS*2を完全に代替するものではない。分散型ネームサービスに登録されているドメイン名が、マルウェアに悪用されたり、主要ブラウザやソフトウェアが認識できなかったりと、利用環境は整備の途上にある。

多数のアドレスやIDを統合的に管理する需要は高く、TLD管理のガバナンスの分散化も進むとみられる。分散型ネームサービスを実効的に利用するには、サイバー攻撃への悪用や不正な書き換えのリスクに備えてシステムの安全性を確保し、複数のTLD管理者が存在することで発生しうる名前衝突を防ぐために他のTLD管理システムとのルール調整を進めるべきと考える。

本レポートでは、分散型ネームサービスの目的を整理し、プロジェクト事例を概観する。また、分散型ネームサービスの課題を踏まえ、分散型ネームサービスの今後を展望する。

1. Top-Level Domain
2. Domain Name System.

目次

1.1 ブロックチェーンのアドレスやドメイン利用の背景

- ブロックチェーンのアドレスは、意味のない長い文字列であり可読性が低い。ユーザの誤入力やアドレスの偽装によって、誤った宛先にデータや暗号資産を送付する可能性が伴う。
- gTLD*1はICANN*2に管理され、一組織に依存するリスクを重くみる流れやTLDに用いる文字列の制限に対する課題感から、より柔軟かつ分権的にドメインを管理する仕組みが構想された。

背景① アドレスの誤読・誤入力

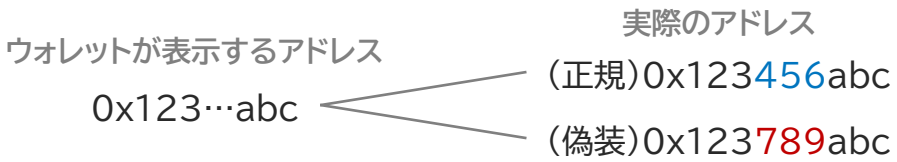
ブロックチェーンのアドレスは、数学的に算出される意味のない文字列であり、その長さは数十文字となっている。

誤読・誤入力による送付ミス防止の必要性

アドレスが覚えづらい/読みづらいことから、ユーザが入力を誤り、意図しない宛先にデータを送付する可能性がある。アドレスの表現形式*2やチェックサム*3など、誤入力を防ぐ仕組みはあるが、正規アドレスか識別はできない。

アドレスポイズニングの防止

アドレスポイズニングとは、ユーザの暗号資産ウォレットに偽装アドレスを潜り込ませ、暗号資産を盗む攻撃。アドレス表記を省略する暗号資産ウォレットで、正規/偽装アドレスが一見して同じ文字列となることを悪用する。



背景② ドメイン管理の集権性

さらなる非中央集権化への期待

2015年以前は、米政府の委託の下でICANNがgTLDを管理*4していた。最終承認権限を一国の政府がもっていて、承認期間も長いため、より柔軟かつ分権的に管理するためのシステムが構想された。

2016年以降、監督権限が政府からICANNに委譲され、複数の委員会の下で管理されている。現在の運用は分散化が進んできたが、一組織に依存するリスクを重要視する流れも依然としてある。

TLD運用の柔軟性

任意のTLDを利用するには、ICANNの審査・承認が必要。

TLD自由化に伴い、2012年以降は任意の文字列のgTLDを申請できるが、個人が利用できるものではない。

(出所)Rajendran, B., Palaniappan, G., Dijesh, R., & Sudarsan, S. D. (2022, July). A Universal Domain Name Resolution Service-Need and Challenges-Study on Blockchain Based Naming Services. In 2022 IEEE Region 10 Symposium (TENSYMP) (pp. 1-6). IEEE.

1. Generic Top-Level Domain. 分野別に割り振る最上位レベルのドメイン名(.com/.netなど)。
2. Internet Corporation for Assigned Names and Numbers. ドメインやIPアドレスなどの管理、DNSルートネームサーバの調整を行う米国の民間非営利法人。
3. アドレスの表現形式(フォーマット)には、BASE58やBech32などがある。BASE58は、+、/、0(数字)、O(大文字)、I(大文字)、l(小文字)の6文字を除く。Bech32は、1、b、i、oの4文字を除くほか、大文字・小文字を区別しない。BASE58はブロックチェーン特有の技術ではない。
4. 入力規則に反していないかを確認する仕組み。
5. ドメインごとにICANNの委託先企業が管理する。

1.2 分散型ネームサービスとは

- 分散型ネームサービス*1とは、ブロックチェーンを用いて名前解決を提供するサービス。
- 背景には、ブロックチェーンをDNSの非中央集権化の手段に用いる流れと、ブロックチェーンのアドレスをはじめとした識別子と任意の名前の対応づけに用いる流れがある。

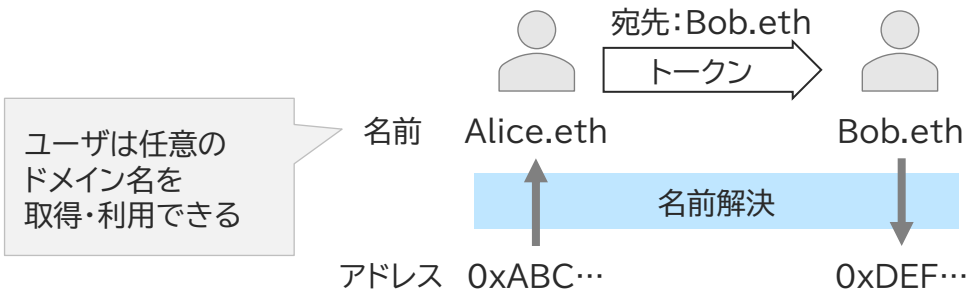
分散型ネームサービスの役割

分散型ネームサービスは、ブロックチェーンを用いて名前解決を提供するサービス。名前解決とは、識別子と任意の名前(ドメイン名)を対応づけることを指す。

従来のDNSで管理されるIPアドレスの名前解決を提供し、DNSの補完を目指すものと、ブロックチェーンのアドレスをはじめとした識別子の名前解決を提供するものに大別される。

名前解決によって、従来のDNSと同様にgTLDを用いたウェブサイトへの接続や新規TLDの提供、ブロックチェーンのトークン*2の送受信などを提供する。

名前解決を用いたトークン送信の例

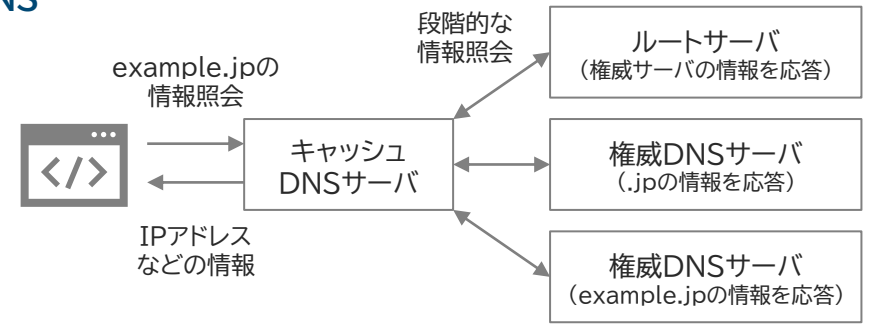


1. ブロックチェーンを用いた名前解決サービスは、Blockchain-based Naming Serviceなどとも呼ばれる。
2. ブロックチェーン上で管理するデータの形式。

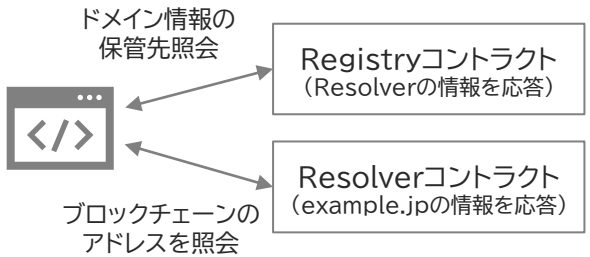
DNSと分散型ネームサービス

DNSとは、IPアドレスとドメイン名の名前解決を提供するシステム。DNSサーバ*3に設定されたドメイン名は、ウェブサイトへの接続やメールの送受信などに用いられる。

DNS



分散型ネームサービス(例:ENS*4)



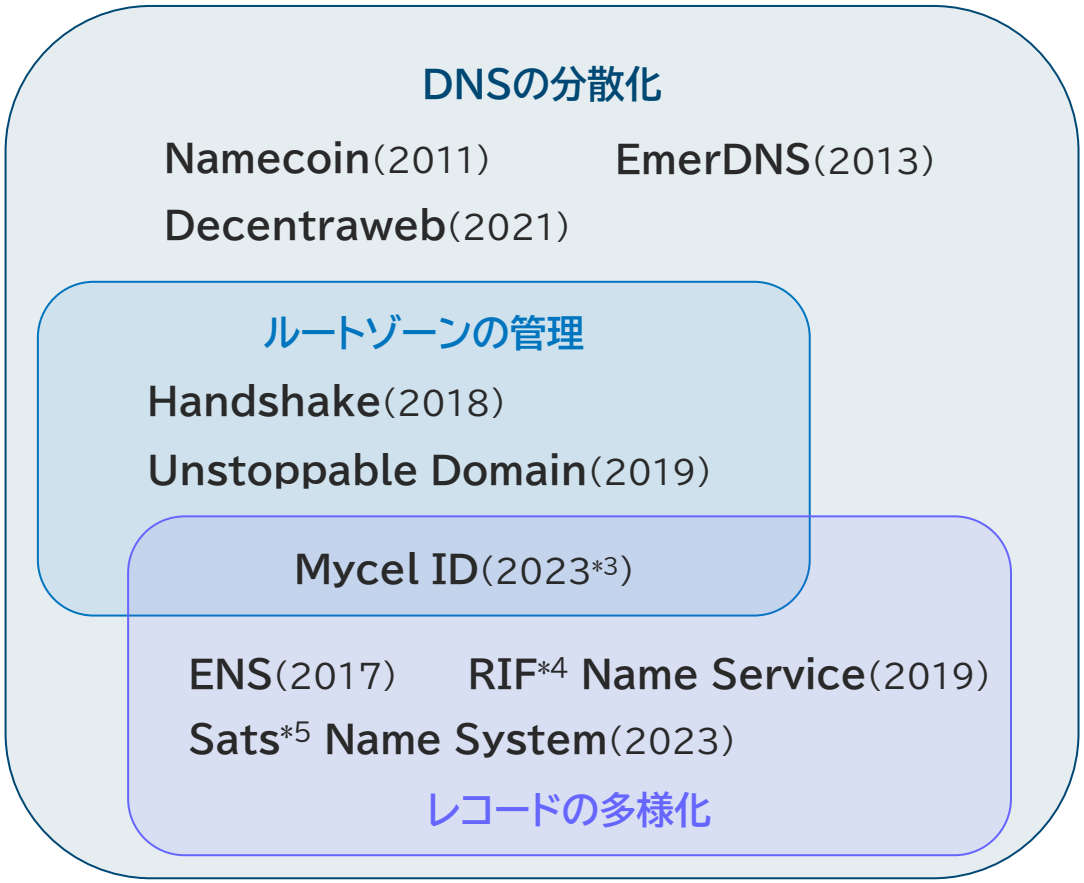
分散型ネームサービスは、名前解決に必要な情報をブロックチェーンに記録し、コントラクトなどを用いて照会する。

(出所)Xia, P., Wang, H., Yu, Z., Liu, X., Luo, X., & Xu, G. (2021). Ethereum name service: the good, the bad, and the ugly. arXiv preprint arXiv:2104.05185.

3. DNSが動作しているコンピュータ。
4. Ethereum Name Service

1.3 分散型ネームサービスの機能

- 分散型ネームサービスは、2011年のNamecoinに始まり、各々のブロックチェーンで構築されてきた。
- ブロックチェーンを用いたDNSサーバの分散化に限らず、ルートゾーン*1の名前空間の管理、ブロックチェーンアドレスの名前解決など、用途はサービスごとに異なる。



DNSの分散化

ICANN管理外のTLDを用いて名前解決を提供する。代表例のNamecoinは、ブロックチェーンにアドレスと任意のSLD(eTLD+1)*2のセットを登録し、専用のブラウザやソフトウェアを経由して名前解決する。

ICANNが管理しないドメインの場合、通常のブラウザやDNSを用いるだけではウェブサイトに接続できない。

ルートゾーンの管理

DNSルートサーバが担ってきた役割を補完する。

ユーザはICANN管理外のTLDを発行できる。

レコードの多様化

ブロックチェーンのアドレスやSNSアカウントなどの名前解決を提供する。既存のDNSと連携、あるいはDNSの機能を実装し、IPアドレスの名前解決を提供するサービスもある。

1. 最上位レベルのドメイン(.com/.netなど)を管理するゾーン。
2. Second-Level Domain. example.comというドメイン名に対し、「.com」がTLD、「example」がSLDに該当する。現状、分散型ネームサービスでは「.co.jp」のようなeTLD(Effective TLD)を利用していないため、eTLD+1がSLDと一致する。
3. テストネット公開時期に基づく。
4. Rootstock (RSK) Infrastructure Framework. EVM(Ethereum Virtual Machine)を用いたBitcoinのサイドチェーンとして登場したRootstock(旧RSK)において、分散型アプリ(DApps)の環境を整える開発者向けフレームワーク。
5. Bitcoinブロックチェーンの最小通貨単位Satoshiに由来する.satsというドメイン名を利用する。

2.1.1 分散型ネームサービス事例｜ENS

- ENS(Ethereum Name Service)は、Ethereumブロックチェーン上のアドレスの名前解決を提供する。
- アドレスの代わりにドメイン名を指定してトークンを送受信できるほか、分散型ファイルシステム上に構築されたWebサイトのアドレスとしても利用できる。

提供開始	2017年	**ブロックチェーン基盤**	Ethereum
開発者・運営者	True Names LTD(Ethereum財団から委譲)		
対応TLD	既存TLD、独自TLD(.eth)		

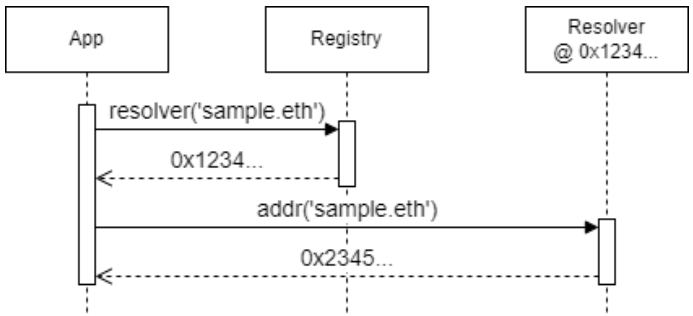
概要

Ethereumアドレスを任意のSLDに紐づける。ドメイン名をNFT*1で管理し、NFTを移転するとドメイン名の所有者を変更できる。DNSSEC*2で保有状況を示せば、アドレスと既存TLDも紐づけられる。

年間契約料*3はドメイン名の長さで変化する。アドレスに加えて、IPFS*4の接続にも対応する。

ENSは3つのコントラクトで構成され、RegistryとResolverを通じ、ドメイン名からアドレスを照会する。

コントラクト	機能
Registry	ドメイン所有者、Resolver、有効期限を管理する。
Resolver	ドメインとアドレス/コンテンツハッシュ*5を対応づける。
Registrar	ドメインの登録・更新処理を実行する。



(出所)ENS Documentation(https://docs.ens.domains)を加工して作成。

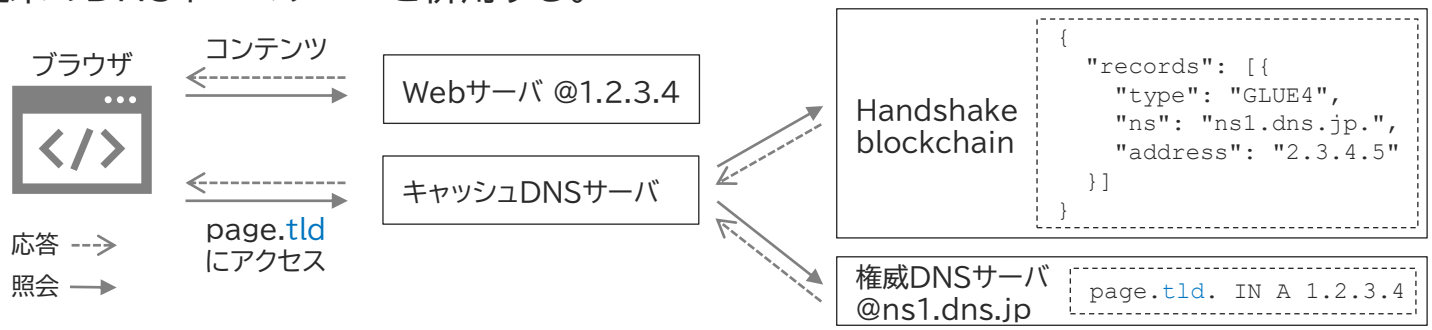
動向

.ethドメインを取得できる外部サービスが登場し、ガス代負担を代理したり、通常のWebサイトのURLとの名前解決を提供したりと、Web2の資源を用いてENSの利便性を高める動きがある。

1. Non-Fungible Token. 互いに識別可能な唯一性のあるトークン。ENSでは、Ethereum上のトークン規格であるERC721,ERC1155が用いられている。
2. DNSレコードの照会元が正式であるか、レコードが改ざんされていないか検証するため、DNSネームサーバに照会する際に電子署名を用いる技術。
3. 3文字で640ドル、4文字で160ドル、5文字以上で5ドル。契約料と別途で、登録にガス代(約30ドル、1ETH=約2,528ドル換算、2024年1月18日時点)が必要。
4. InterPlanetary File System. 分散型ファイルシステムの一つ。
5. IPFSは、コンテンツのハッシュを算出し、このハッシュをID用いてコンテンツの保存先を示す(コンテンツ指向)。HTTPは、URLを用いて保存先を示す(ロケーション指向)。

2.1.2 分散型ネームサービス事例｜Handshake

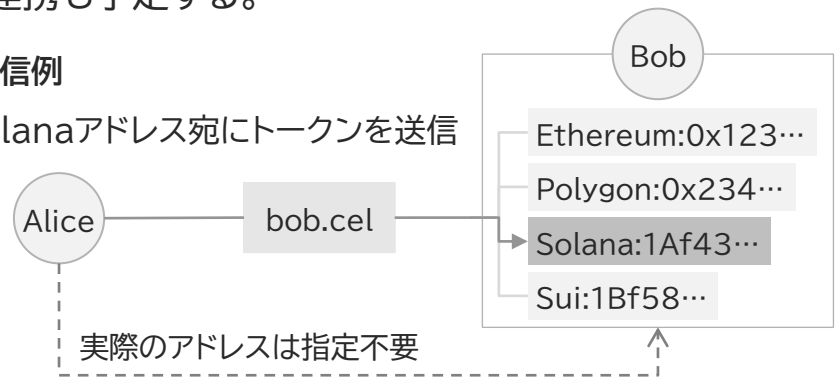
- Handshakeは、ブロックチェーンを用いてルートゾーン*1の名前空間を管理する。ICANNの下でTLDを管理する集権的なDNSや、ドメインの信頼性を担保する認証局を補完・代替する構想を掲げる。
- 1,000万件以上のTLDが登録済みとなっているが、実際に利用されている事例は少ない。

提供開始	2018年	**ブロックチェーン基盤**	bcoin*2ベースのブロックチェーン
開発者・運営者	Handshakeコミュニティ		
対応TLD	任意のTLD（既存TLDや特定の企業名を除く*3）		
概要	任意のTLDを発行し、DNSと同様のリソースレコード（DS, NS, TXT, GLUE4/6）*4とSYNTH4/6*5を割り当てる。Handshakeブロックチェーンは、従来のDNSルートサーバの役割をもち、Handshakeが管理するTLDの名前解決を提供する権威DNSサーバの情報を提供する。 ブロックチェーンに記録する情報はルートゾーンの名前に限るため、Web/メールサーバと紐づけるには従来のDNSネームサーバを併用する。  （出所）「Handshake Resource Record Guide」Handshake Developer Documentation. https://hsd-dev.org/guides/resource-records.html（閲覧日：2024年2月29日）		
動向	登録済みのTLDは約1,230万件（2024年1月時点）*6だが、実際に利用されているものは少ない。		

1. 最上位レベルのドメイン名（.com/.netなど）を管理するゾーン。
2. Bitcoinのシステムを JavaScriptベースで実装したブロックチェーン。
3. 予約済みドメイン名はリポジトリ（https://github.com/handshake-org/hs-names）を参照。
4. DSレコードは、DNSSECにおいて子ゾーンの公開鍵の正しさを保証するレコード。GLUE4/6レコードは、ネームサーバのドメインとIPv4/6アドレスを対応させるレコード。
5. IPv4/6アドレスのみ設定することでGLUEレコードを自動生成するレコード。ブロックチェーンに記録するデータサイズを減らす効果がある。
6. Namebase調べ（https://www.namebase.io/stats/, 閲覧：2024/2/9）

2.1.3 分散型ネームサービス事例｜Mycel ID

- Mycel IDは、複数のブロックチェーン間で利用できるデジタルIDの名前解決を提供する。
- 任意のTLD/SLDを用いて、各ブロックチェーンのアドレスやDNSレコード、IPFSのアドレスなどを個別に指定せずに名前解決し、直感的に操作できるインフラを目指す。

提供開始	2023年*1	**ブロックチェーン基盤**	Tendermint*2ベースのブロックチェーン
開発者・運営者	Mycel		
対応TLD	独自TLD(.cel)、既存TLDにも対応予定		
概要	ユーザが直感的に操作できるインフラ*3の構築を目的とし、その一つとしてデジタルID基盤を提供する。 ユーザは任意のTLD/SLDを取得できる。複数のブロックチェーン間で相互に利用することを想定し、Ethereumや他のEVM*4互換ブロックチェーン、ブロックチェーン間通信(IBC*5)対応ブロックチェーンで動作する。また、他の分散型ネームサービスとの連携も予定する。 名前解決の対象はブロックチェーンのアドレスに限らず、DNSレコードやIPFSのアドレスなども含まれる。 **トークン送信例** BobのSolanaアドレス宛にトークンを送信  		
動向	2023年7月、SHUGYOテストネットを公開した。Aptos, Bitcoin, Ethereum, Polygon, Solana, Suiブロックチェーンのアドレスに対応している*6。		

1. テストネット公開時期に基づく。
2. ブロックチェーンでの合意形成を実装するソフトウェアの一種。
3. Mycelでは、これをIntent-Centric Infrastructureと呼ぶ。UX向上のため、ユーザがブロックチェーン上の複雑な処理(Transaction)を理解して指示を出すのではなく、ユーザが意図した結果が得られるように状態遷移させるという設計思想(Intent-Based Architecture)に基づく。
4. Ethereum Virtual Machine. ブロックチェーンの状態管理やプログラム実行を行うエンジン。
5. Inter-Blockchain Communication
6. アルファベット順。

2.2 現状の課題

- ドメイン名の利用者が不明瞭であることから、サイバー犯罪に悪用される事例がみられる。
- 複数のTLD管理者が存在することで名前衝突が発生したり、分散型ネームサービスに登録されたTLDを主要ブラウザやソフトウェアが認識できないなど、利用環境は整備の途上にある。

サイバー犯罪への悪用

Namecoin

同サービスは「.bit」ドメインの名前解決を提供しているが、マルウェアの悪用が多くみられた。

分散型ネームサービスの多くは、暗号資産とブロックチェーンのアドレスがあればドメイン名を取得できるため、犯罪に悪用されても利用者を特定することは難しい。

代表的なドメイン管理プロジェクトの一つ「OpenNIC*1」は、2019年に同TLDの対応を終了した。

EmerDNS

Namecoinと同様に、マルウェアへの悪用がみられる。

Windowsシステムに侵入し、バックドアを仕掛けるなどの攻撃を行うBazarマルウェア*2の存在が確認されている。

利用環境の未整備

分散型ネームサービスを利用すれば、サービス独自のTLDや任意のTLDを利用できる一方、既存環境との整合性がないことから、自由に利用できない現状がある。

名前空間における一意性の担保

ICANNがTLDを管理しているが、より柔軟にTLDを運用するため、過去にも代替TLDシステム*3が登場してきた。

複数のTLD管理者が存在する場合、一つのドメインが複数の宛先を示しうる（名前衝突）。

ブラウザやソフトウェアは対応途上

ユーザが、Webサイトのドメイン名として新規TLDを登録しても、ChromeやEdge、Firefoxなど主要ブラウザは、TLDを認識できない。

専用ブラウザやHTTPゲートウェイ経由で接続する必要がある。例として、ENSはCloudflare*4と連携し、ENSの名前に「.link」を付与してWebサイトへの接続に対応している。

1. ICANNなどのTLD管理・運用者（レジストリ）に代わり、ユーザ主導でTLDを管理するプロジェクト。（NIC: Network Information Center）
2. EmerDNSが利用しているTLD（.bazar）に由来する。
3. alternate rootsと呼ばれる。OpenNICもその一つ。
4. CDN（Contents Delivery Network）を提供する米企業。

3.1 今後の展望・考察

①多数のアドレスやIDを統合的に管理する需要は高い

ブロックチェーンでは、各システムの仕様にしたがったアドレスを発行している。ユーザは、接続中のネットワークを認識し、その使い分けが求められているのが現状。基盤として広く用いるには、ユーザリテラシーに依存した設計は現実的ではない。

ブロックチェーンを含む分散型台帳システムを基盤に用いた分散型識別子（DIDs[*1]）の検討も進んでいる。現在公開されている仕様案によると、DIDsもブロックチェーンのアドレスと同様に可読性の低い文字列になる可能性が高く、セキュリティ強化やUX向上の解決案の一つとして名前解決の需要が存在する。

②TLD管理のガバナンスの分散化

歴史的背景から、米国商務省がICANNに委託する形でTLDやIPアドレスなどのインターネット資源を管理してきたが、2016年に監督権限を委譲した。現在は、ICANNの下で各委員会が監督する。

インターネットは、自律・分散・協調を理念として掲げる。インターネット資源の監督権限は民間に移管され、全世界の社会基盤として拡大するとともに、特定の国・政府に依存しない運営に変わってきた。

分散型ネームサービスは、ICANNが担うTLD管理を補完するだけでなく、サービスを監督する機能を分散できる。既にENSはブロックチェーンを用いて非中央集権的な運営を実現する分散型自律組織（DAO[*2]）の仕組みを導入している。他の分散型ネームサービスにおいても、同様の傾向が続くとみられる。

1. Decentralized Identifiers. 2022年7月、W3CがDIDs v1.0の仕様を策定した。
2. Decentralized Autonomous Organization.

3.2 分散型ネームサービスを構築・利用するうえでの提言

①システムの安全性確保が最重要

基盤として活用するには、安全性の確保が最重要となる。近年DNSハイジャック*1が多発し、既存のDNSはドメイン管理の体制強化を進めている。分散型ネームサービスの主な用途には、ブロックチェーンのアドレスの名前解決があるが、ドメイン名の所有状態を書き換えれば暗号資産の窃取につながる。

管理の分散性が強みである一方、サイバー攻撃への悪用や不正な書き換えが生じた際に対策を講じる必要がある。具体的には、不正利用が確認されたドメイン名の凍結や所有の解除に関する実装、脆弱性をついた書き換え*2を防ぐためのスマートコントラクトの監査強化などが想定される。

②既存のDNSや他の分散型ネームサービスとの連携を強化

複数のTLD管理者が存在する場合、名前衝突によって意図しない宛先に接続したり、トークンを送信したりする可能性がある。代替TLDシステムの登場によって、ドメイン名の一意性を担保できなくなるという問題は以前から議論されていて、分散型ネームサービスがTLDを管理する場合も同様のリスクが伴う。

ICANNでは、名前衝突が発生した際に衝突を通知し対策を求めるためのフレームワーク*3を運用している。また、Sats Name Serviceでは、最も先に登録されたドメイン名を有効とする仕組み*4を採用している。

複数のサービスでTLDが登録された場合、どのドメイン名を正規のものとみなす、あるいは優先するべきか共通認識が必要である。

1.他者のDNSに侵入し、リソースレコードを書き換えて偽サイトに誘導する攻撃。ドメイン管理サービスへの不正ログインやレジストリへの不正アクセス・書き換え、キャッシュDNSサーバ情報の書き換えなどの手法がある。
2.ENSでは、整数のオーバーフローによって登録済みドメイン名の有効期限を短縮させるという脆弱性「CVE-2023-38698」が発見された事例がある。
3.Name Collision Occurrence Management Framework. ICANNが名前衝突を発見した場合、レジストリオペレータに対して該当ドメイン名の名前解決先にループバックアドレスを設定するよう求める。
4.First-is-first ruleと呼ばれる。

まとめ

現状

分散型ネームサービスとは、ブロックチェーンを用いてIPアドレスやブロックチェーンのアドレスなどとの名前解決を提供するサービス。ブロックチェーンのアドレスの可読性が低いことや、現在のTLD管理の中央集権性に対する課題感から、ブロックチェーンでのドメイン名管理が構想された。

IPアドレスの解決を提供するサービスもあるが、DNSを完全に代替するものではなく、一部TLD/SLDの管理に用いられる。分散型ネームサービスに登録されているドメイン名が、マルウェアに悪用されたり、主要ブラウザやソフトウェアが認識できなかったりと、利用環境は整備の途上にある。

展望

①多数のアドレスやIDを統合的に管理する需要は高い

ユーザは、各システムの仕様をある程度理解し、使い分けを求められる。基盤として広く用いるにはユーザリテラシーに依存した設計は現実的でなく、セキュリティやUXの観点で需要が見込まれる。

②TLD管理のガバナンスの分散化

分散型ネームサービスは、ICANNが担うTLD管理を補完するだけでなく、サービスを監督する機能をDAOで分散でき、運営の分散化が続くとみられる。

提言

①システムの安全性確保が最重要

ブロックチェーンのアドレスの名前解決において、ドメイン名の所有状態を書き換えれば、暗号資産の窃取も可能。サイバー攻撃への悪用や不正な書き換えが生じた際に対策を講じる必要がある。

②既存のDNSや他の分散型ネームサービスとの連携を強化

複数のTLD管理者が存在する場合、ドメイン名の一意性を担保できなくなる。複数のサービスでTLDが登録された場合、どのドメイン名を正規のものとみなす、あるいは優先するべきか共通認識が必要。