Introducing a Blockchain-Based Domain Name System (BDNS)

Alexander Hofstätter, Wirtschaftsuniversität Wien, 23.10.2018

Implementierung eines blockchainbasierten Domain Name Systems zur Eliminierung von Vertrauen in zentrale Instanzen sowie zur Sicherstellung von freiem Internetzugang.

Das Problem

Aktuell besteht DNS aus mehreren zentralen, kommerziell betriebenen Servern sowie 13 weltweiten Root Severn, wessen Betrieb von der ICANN (Internet Corporation for Assigned Names and Numbers) koordiniert wird. Das DNS System und deren hierarchisch angeordnete DNS Server sind zuständig für die Auflösung von Domain-Namen (*wu.ac.at*) in die zugehörigen IP-Adressen (z.B. *137.208.2.10*) unter welcher der tatsächliche Server (z.B. Webserver) technisch erreicht werden kann.

DNS ist daher wesentlich für alle modernen Systeme, Anwendungen, IT Systeme und Apps (überall dort, wo Netzwerkkommunikation involviert ist). In jüngerer Vergangenheit wurden zentrale, dominierende DNS Server (z.B. Server von Internet Service Providern) angegriffen und dazu missbraucht, falsche DNS Einträge auszuliefern um so den gesamten Netzwerkverkehr auf andere, vom Angreifer kontrollierte, Systeme umzuleiten. So passiert bei z.B. MyEtherWallet.com im April 2018, wo der zuständige DNS Dienst Route 53 (Teil von Amazon Web Services) angegriffen wurde. User wurden auf infizierte Server umgeleitet und gaben dort ihre Private Keys preis.

DNS basiert also maßgeblich auf Vertrauen in zentrale, große Instanzen, welche oft primär kommerzielle Leitbilder verfolgen, Interessenkonflikten unterliegen oder sogar unter dem Einfluss staatlichen Zwangs stehen (Great Firewall von China; Blockierung von Twitter in der Türkei 2014).

Die Lösung

Das Einsetzen der Blockchain Technologie, soll wie beim Bitcoin das Vertrauen in zentrale Einheiten eliminieren und durch viele weltweite Netzwerkteilnehmer, welche vollständiges Datenmaterial (Domain-Name und zugehörige IP-Adresse) zu allen verfügbaren Einträgen vorweisen, unabhängig sind sowie von jedem Individuum betrieben werden können, gestützt werden.

Technisch kann bei der Umsetzung dieser Idee auf die Verwendung von zwei Blockchains zurückgegriffen werden. Eine Blockchain für die Speicherung aller Full Nodes, eine eher kleinere Datenmenge. Diese soll vor allem den anfragenden Clients (Light Nodes) dienen und eine Speicherung von großen Datenmengen (aller Name-Tabellen) umgehen. Eine zweite Blockchain würde primär unter den Full Nodes aufgebaut werden, welche die tatsächlichen Domain-IP Tabellen enthalten. Die Verwendung einer zweiten (Light Node Blockchain) soll die Verbindung zu den Full Nodes absichern sowie eine Reduzierung der notwendigen Datenmengen auf den Light Nodes herbeiführen.

Verfügbarkeit. BDNS garantiert die weltweite Verfügbarkeit von DNS Einträgen. Die Key-Value-Daten sind allen Teilnehmern des Netzwerks bekannt und durch die Kenntnis vieler verteilter Netzwerkteilnehmer kann via P2P Verbindungen die gesamte Liste und Historie der DNS Datenbank angefordert werden.

Transparenz. Durch die Eliminierung zentraler Instanzen kann der IP-Verlauf einer jeden Domain erhoben werden und offengelegt werden. Dies kann u.a. zur Aushebung vergangener Einträge und zur Sicherstellung von Domain-Reputation verwendet werden.

Misstrauen. Durch BDNS können DNS Einträge von beliebigen, unbekannten Netzwerkteilnehmern verarbeitet werden, sie müssen lediglich gegen allgemein gültige Regeln verifiziert werden. Es entfällt das Vertrauen in zentrale, autoritäre DNS-Server und deren Betreiber.

Freiheit. Durch das Nutzen der technischen und kryptografischen Möglichkeiten kann der freie Zugriff auf alle Inhalte für jedermann sichergestellt sowie Zensur durch technische Nicht-Durchführbarkeit entgegen gewirkt werden. **Freedom by Design**.

Herausforderungen

Kompatibilität. Da DNS erstmals 1983 entworfen und mittlerweile u.a. in den RFC (Request for Comments) 1034 und 1035 standardisiert ist und daher in de facto allen Systemen fester Bestandteil und exakt nach Standard implementiert. Um die Verbreitung zu fördern muss ein BDNS Protokoll entwickelt werden welches gewissermaßen kompatibel zum bisherigen DNS Standard ist.

Big Player. Aktuell sind viele zentrale Instanzen involviert, welche das hierarchische Pyramidenschema "anführen". Big Player sind z.B. Betreiber von Root-Server, ISPs, Domain Registrare (NICs) aber auch Staaten. All diese Akteure setzen maßgeblich Standards für DNS Systeme und dürften schwer von einem nutzerorientierten BDNS Standard zu sein. Eine communitybasierte und tatsächlich dezentrale Variante eines solchen Systems würde diesen Big Player die Macht nehmen und deren wirtschaftlichen Interessen entgegen wirken.

Zugriffskosten. Momentan ist der Lesezugriff auf DNS Informationen sehr einfach und insbesondere kostengünstig möglich (de facto: kostenlosem einfache IP basierte Abfrage). Hier müssen Möglichkeiten gefunden werden um diese Kosteneffizienz bei Lese- und Schreibzugriffen auch in einem blockchainbasierten System zu gewährleisten.

Vorhandene Technologien. Aktuell vorhandene Technologien und Entwicklungen schaffen primär neue Domain-Endungen (TLDs) wie z.B. *.bit* zur Nutzung in einem begrenzten Rahmen. Da die Mehrheit der Kommunikationswege auf den herkömmlichen TLDs basiert, ist das Ziel dieser Idee die Schaffung eines kompatiblen BDNS zur Implementierung eines globalen Systems für bestehende Domains.