Independent Submission
Request for Comments: 9518
Category: Informational
ISSN: 2070-1721

M. Nottingham
December 2023

Centralization, Decentralization, and Internet Standards

Централизация, децентрализация и стандарты Internet

Аннотация

В этом документе рассматриваются аспекты централизации, связанные с разработкой стандартов Internet. Утверждается, что, несмотря на ограниченность возможностей предотвращения многих форм централизации, остаётся возможным внести вклад, способствующий децентрализации Internet.

Статус документа

Документ не относится к категории Internet Standards Track и публикуется для информации.

Это вклад в RFC Series, независимый от других потоков RFC. RFC Editor принял решение о публикации документа по своему усмотрению и не делает каких-либо заявлений о его ценности для реализации или внедрения. Документы, одобренные для публикации RFC Editor, не претендуют на статус Internet Standard (см. раздел 2 в RFC 7841).

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc9518.

Оглавление

1. Введение

Одним из определяющих свойств Internet является отсутствие единой точки технического, политического или экономического контроля. Возможно именно это свойство способствовало начальному распространению Internet и широте охвата. Для подключения, внедрения приложений или использования Internet с определёнными целями не требуется разрешение, поэтому возможно удовлетворение различных потребностей и применение в разных условиях.

Хотя сохранение такого состояния остаётся широко поддерживаемой целью, согласованное сохранение во всем спектре услуг и прложений, который люди воспринимают как Internet, оказалось труднодостижимым. Если ранние службы, такие как сетевые новости (Network News Transfer Protocol или NNTP) и электронная почта, имели множество взаимодействующих провайдеров, то многие современные платформы для содержимого и услуг управляются одной коммерческой структурой без какого-либо совместимого варианта. Некоторые из них стали настолько распространёнными и важными, что многие стали считать их синонимом Internet [Komaitis].

Эти сложности вызывают вопрос о роли, которую следует играть разработке архитектуры, в частности, выполняемая под эгидой таких органов стандартизации, как IETF, в контроле за централизацией Internet.

Этот документ утверждает, что, несмотря на необходимость децентрализованных стандартов для предотвращения централизации функций Internet, этого может оказаться недостаточно для достижения цели, поскольку централизация зачастую вызывается нетехническими факторами, не контролируемыми органами стандартизации. Поэтому органам стандартизации не следует зацикливаться на предотвращении всех форм централизации, им следует предпринимать действия по обеспечению возможности децентрализованной работы принимаемыми ими спецификациями.

Хотя этот документ широко обсуждался в сообществе IETF (см. раздел благодарностей), он отражает точку зрения автора, а не согласованный взгляд сообщества. Документ предназначен, прежде всего, инженерам, разрабатывающим и стандартизующим протоколы Internet. Разработчики фирменных (proprietary) протоколов и приложений также могут извлечь пользу из рассмотрения этих вопросов, особенно если они намерены предоставить свои разработки для последующей стандартизации. Разработчики правил (политики) могут использовать документ для характеризации нарушений, вносимых централизованными протоколами и приложениями, и оценки предлагаемых мер по их устранению.

В разделе 2 приведено определение централизации и разъяснено, почему она зачастую нежелательна, и рассмотрены проявления централизации в Internet. В разделе 3 рассматривается децентрализация и выделены некоторые стратегии и их ограничения. Раздел 4 рассматривается роль стандартов Internet в контроле централизации, а раздел 5 посвящён будущим направлениям работы.

2. Централизация

В этом документе централизацией называется положение дел, когда один субъект или небольшая группа может монопольно (исключительно) наблюдать, фиксировать (capture), контролировать или получать ренту от работы или использования функций Internet. Субъектом (entity) в данном случае может быть один человек, группа или корпорация. ACK organization might be subject to governance that mitigates centralization risk (see Section 3.1.3), but that organization is still a centralizing entity.

Термин «функция Internet» применяется в этом документе в широком смысле. В самом прямом смысле это может used broadly in this document. Most directly, it might be an enabling protocol already defined by standards, such as IP [RFC791], BGP [RFC4271], TCP [RFC9293], or HTTP [HTTP]. It might also be a proposal for a new enabling protocol or an extension to an existing one.

Because people's experience of the Internet are not limited to standards-defined protocols and applications, this document also considers centralization in functions built on top of standards -- for example, social networking, file sharing, financial services, and news dissemination. Likewise, the networking equipment, hardware, operating systems, and software that act as enabling technologies for the Internet can also impact centralization. The supply of Internet connectivity to end users in a particular area or situation can exhibit centralization, as can the supply of transit between networks (so called "Tier 1" networks).

This definition of centralization does not capture all types of centralization. Notably, technical centralization (for example, where a machine or network link is a single point of failure) is relatively well understood by engineers; it can be mitigated, typically by distributing a function across multiple components. As we will see, such techniques might address that type of centralization while failing to prevent control of the function falling into few hands. A failure because of a cut cable, power outage, or failed server is well understood by the technical community but is qualitatively different from the issues encountered when a core Internet function has a gatekeeper.

Likewise, political centralization (for example, where a country is able to control how a function is supplied across the whole Internet) is equally concerning but is not considered in depth here.

Even when centralization is not currently present in a function, some conditions make it more likely that centralization will emerge in the future. This document uses "centralization risk" to characterize that possibility.

2.1. Централизация может быть вредной

Многие инженеры, участвующие в разработке стандартов Internet, стремятся предотвратить централизацию и противодействовать ей, поскольку считают централизацию несовместимой с историей и архитектурой Internet. Будучи «большим разнородным набором соединённых сетей» [BCP95], Internet часто характеризуется как «сеть сетей», где операторы выступают как партнёры (peer), согласные упростить взаимодействие, а не исполнители чужой воли. Такая ориентация на независимость превалирует в устройстве Internet, например, в виде концепции автономных систем.

Нежелание мириться с централизацией обусловлено также множеством перечисленных ниже потенциально вредных эффектов.

Power Imbalance - дисбаланс власти

Когда третья сторона получает неизбежный доступ к коммуникациям, она обретает информационные и позиционные преимущества, позволяющие наблюдать за поведением (паноптикум) формировать и даже отклонять его (точка удушения), которые могут использованы этой стороной (или имеющим над ней власть государством) в целях принуждения [FarrellH] и даже разрушения самого общества. Подобно эффективному управлению штатами США [Madison], эффективное управление Internet требует, чтобы власть над любой функцией не была сосредоточена в одном месте без соответствующего сдерживания и противовесов.

Limits on Innovation - ограничения для инноваций

Сторона, контролирующая коммуникации может исключить возможность «инноваций без разрешения», т. е. возможность внедрения новых, непредусмотренных приложений без согласования со сторонами, не участвующими непосредственно в конкретных коммуникациях.

Constraints on Competition - ограничения для конкуренции

Internet и пользователи этой сети выигрывают от здоровой конкуренции, когда приложения и услуги доступны от множества поставщиков на основе совместимых стандартов. Когда требуется использовать централизованные услуги или платформы по причине отсутствия подходящей замены, они фактически становятся важнейшими элементами, что открывает возможности для злоупотреблений.

Reduced Availability - снижение доступности

Доступность Internet (а также приложений и услуг в сети) повышается при наличии множества вариантов доступа. Хотя уровень доступности может повышаться в результате целенаправленных действий крупного централизованного провайдера, отказ такого провайдера может оказывать чрезмерное влияние на доступность.

Monoculture - монокультура

Зона действия (масштабы) централизованного провайдера может повышать роль незначительных недостатков в функциях до такой степени, что они будут приводить к серьёзным последствиям. Например, единая база кодов для маршрутизации повышает влияние ошибок и уязвимостей, а один алгоритм рекомендаций для содержимого может иметь серьёзные социальные последствия. Разнообразие реализаций функций ведёт к росту устойчивости при системном рассмотрении, поскольку «прогресс - это результат эволюционного процесса проб и ошибок множества свободно взаимодействующих между собой агентов» [Aligia].

Self-Reinforcement - самоусиление

Как отмечено многими (см., например, [Abrahamson]), доступ централизованного провайдера к данным позволяет ему улучшать свои предложения, отказывая в таком доступе другим.

Взаимосвязи между этими вредными факторами и централизацией зачастую сложны. Централизация не всегда вызывает вредные последствия, а при их наличии не всегда имеется прямой и простой компромисс. Рассмотрим, например, связь между централизацией и доступностью. Система с централизованным управлением может быть более доступной за счёт наличия у крупного оператора больших ресурсов, но при возникновении отказа зона охвата будет больше. Децентрализованные системы могут быть более устойчивыми к некоторым формам отказов, но менее устойчивыми к другим. Например, они могут менее способны реагировать на системные проблемы и подвержены большему числу уязвимостей защиты в целом. Поэтому нельзя сказать, что централизация снижает доступность во всех случаях, равно как нельзя сказать, что она всегда повышает доступность.

Это противоречие можно наблюдать в таких областях, как облачные технологии и мобильный доступ в Internet. Если популярный провайдер облачного хостинга становится недоступным (по техническим или иным причинам), работа многих пользователей Internet может быть нарушена (особенно при наличии множества зависимостей у современных web-сайтов, см. [Kashaf]). У крупного поставщика услуг доступа в Internet может возникнуть отказ, затрагивающий сотни тысяч пользователей (и более) точно так же, как ранее проблемы у крупных телефонных компаний приводили к масштабным отключениям [PHONE]. В обоих случаях услуги не являются технически централизованными и у операторов имеются серьёзные стимулы для резервирования и применения различных средств снижения риска отказа одного компонента. Однако в целом операторы полагаются на единую базу кода, ограниченный набор оборудования, единую плоскость управления и все они могут стать причиной широкомасштабных отказов.

Если бы у этих услуг был лишь один поставщик (как в старых телефонных системах), их можно было бы считать централизованными в части влияния на доступность. Однако похожие услуги предлагает множество облачных провайдеров и в большинстве мест имеется не один оператор мобильной связи. Это ослабляет аргумент о связи централизации с доступностью, поскольку пользователи могут переключиться на другого провайдера или пользоваться услугами нескольких провайдеров одновременно (см. параграф 4.4). Это наводит на мысль о том, что при рассмотрении взаимосвязи между централизацией и доступностью данной функции нужно выяснить, какие существуют препятствия для переключения на другого провайдера (что делает влияние отказов временным и преодолимым) или одновременной работы с несколькими провайдерами (для маскировки отказа одного провайдера).

Другим примером необходимости учёта нюансов является оценка конкурентных ограничений. Хотя повышение конкурентоспособности предоставления различных функций Internet может быть стимулом для многих инженеров, только суды (иногда регуляторы) имеют полномочия определять соответствующий рынок и оценивать допустимость того или иного поведения в плане конкуренции. В частности, концентрация рынка не всегда говорит о проблемах конкуренции, поэтому то, что техническое сообщество считает нежелательной централизацией, не всегда является нарушением антимонопольных правил или законов.

2.2. Централизация может быть полезной

Перечисленные выше вредные последствия централизации широко известны. Менее изучена зависимость функциональности некоторых протоколов и приложений от централизации. Централизация зачастую обусловлена технической необходимостью. Например, единый глобально координируемый «корень доверия» (source of truth) является централизованным по своей природе. Примером является корневая зона системы доменных имён (Domain Name System или DNS), которая позволяет преобразовывать понятные человеку имена в сетевые адреса согласованным в глобальном масштабе способом.

Другим примером является распределение адресов IP. Для маршрутизации Internet требуется распределение уникальных адресов, но если одно правительство или компания захватит управление распределением адресов, вся сеть Internet окажется под угрозой злоупотреблений со стороны этой организации. Модель доверия в Web требует наличия удостоверяющего центра (Certificate Authority или CA) в качестве корня доверия при обмене данными между браузерами и серверами, что влечёт за собой риск централизации, который нужно учитывать при создании системы.

Протоколы, которым нужно решать «проблему встречи» (rendezvous problem) для согласования взаимодействия между двумя сторонами, не находящимися в посредственном контакте, тоже требуют централизации. Например, протоколам чата нужно согласование между сторонами, которые хотят «поговорить». Хотя фактическое взаимодействие может происходить напрямую (если протокол это позволяет), для обнаружения конечными точками друг друга на определённом этапе обычно нужна третья сторона. С точки зрения пользователей с этим связан риск централизации.

И даже при отсутствии острой необходимости централизация может приносить пользу участникам взаимодействия и сообществу. Например, давно известно, что повышение эффективности за счёт экономии, связанной с масштабом, может приводить к централизации [Demsetz]. Эта эффективность может быть передана пользователям как продукция более высокого качества за меньшую цену и может также позволить реализацию функций, которые нежизнеспособны в меньшем масштабе.

Комплексные и рискованные функции, такие как финансовые услуги (например, обслуживание кредитных карт), часто концентрируются в небольшом числе специализированных организаций, где для их реализации имеется необходимый опыт и возможности.

Централизация может также обеспечивать возможность полезного контроля. В [Schneider2] отмечено: «Централизованные структуры могут обладать достоинствами вроде предоставления общественности возможности сосредоточить своё внимание на надзоре или формирования властного блока, способного противостоять менее контролируемым блокам, которые могут возникать. Централизованные структуры, заслужившие широкое признание в последние столетия, включая правительства, корпорации и некоммерческие организации, достигли этого в немалой степени благодаря их продуманному устройству».

Можно видеть, когда для функции требуется управление, чтобы реализовать общие цели и защитить интересы меньшинства. Например, функции модерации содержимого навязывают ценности сообщества, которые многие считают преимуществом. Конечно, их можно рассматривать как «дроссельную заслонку» (choke point), на которую можно возложить неприемлемые меры контроля, если для этого механизма управления нет должного надзора, «прозрачности» и подотчётности.

В конечном счёте решение о пользе централизации является субъективным. Некоторые протоколы не могут работать без централизованной функции, другие могут получить в некоторых случаях значительную пользу от централизации. Хотя централизация в целом вызывает наибольшее беспокойство, когда она не считается необходимой и полезной, когда у неё нет требуемых сдержек, противовесов или иных механизмов подотчётности, когда централизация создаёт «фаворитов», которых трудно (или невозможно» вытеснить, а также в случаях угроз архитектурным свойствам, обеспечивающим успех Internet.

3. Децентрализация

Хотя термин «децентрализация» имеет долгую историю использования в экономике, политике, религии и международных отношениях, в [Baran] дано одно из первых определений, относящихся к компьютерным сетям, как условия, когда: «не требуется во всех случаях полагаться на одну точку».

Техническая централизация изучена относительно хорошо, хотя и является нетривиальной темой. Избежать любой формы централизации, включая нетехнические, с использованием лишь технических средств (включая разработку протоколов) достаточно сложно и здесь возникает несколько проблем.

Первая и наиболее важная проблема связана с тем, что технические меры децентрализации в лучшем случае имеют ограниченное влияние не нетехнические формы централизации. Согласно [Schneider1], «децентрализованная технология сама по себе не гарантирует децентрализованных результатов». Как показано ниже в параграфе 3.1, технические меры лучше считать необходимыми, не недостаточными для полной децентрализации функции.

Во-вторых, для децентрализации функции требуется решение проблем, с которыми не сталкиваются централизованные функции. Децентрализованные функции сложнее адаптировать к потребностям пользователей (например, внедрять новые функции или экспериментировать с пользовательским интерфейсом), поскольку это часто требует согласования действий множества участников [Marlinspike]. Для централизованных функций более доступна экономия за счёт масштаба, а также данные, которые можно использовать для доработки функций. Эти факторы делают централизованные функции более привлекательными для поставщиков услуг, а в некоторых случаях могут делать децентрализованные решения нерентабельными.

В-третьих, определение аспектов функции, которые следует децентрализовать, может оказаться сложным из-за наличия множества взаимодействий между различными типами и источниками централизации, а также потому, что централизация становится очевидной лишь после масштабного развёртывания функции. Усилия по децентрализации часто приводят лишь к переносу централизации в другую точку, например, в управление, реализацию, внедрение или вспомогательные функции. Например, на ранних этапах существования среда Web представлялась и планировалась как децентрализованная и потенциал централизации стал очевиден лишь после того, как крупные сайты успешно использовали сетевые эффекты (и добились законодательного запрета функциональной совместимости, повысившего стоимость переключения, см. [Doctorow]) для достижения доминирования в социальных сетях, торговых площадках и аналогичных функциях.

В-четвёртых, у разных сторон могут быть добросовестные разногласия в части понимания достаточности децентрализации, основанные на убеждениях, представлениях и целях. Как централизация, так и децентрализация не являются дискретными процессами (континуум) и не все согласны с определением «верного» уровня или типа, а также соотнесением разных форм централизации друг с другом или архитектурными целями (например, безопасностью и приватностью). Эти противоречия можно проследить на примере DNS. Хотя некоторые аспекты системы децентрализованы (например, распределение функции поиска между локальными серверами, которые пользователь может задавать), основным аспектом централизации DNS является работа системы в качестве пространства имён - единой глобальной «точки доверия» с присущей (хотя и выгодной) централизацией управления. ICANN смягчает связанные с этим риски за счёт управления с участием множества заинтересованных сторон (см. параграф 3.1.3). Хотя многие считают такой механизм достаточным и даже обладающим желаемыми качествами (например, возможность навязывать стандарты сообщества в части работы пространства имён), другие отвергают надзор ICANN за DNS как незаконный, отдавая предпочтение децентрализации на основе протоколов распределенного согласия перед управлением людьми [Musiani].

В-пятых, децентрализация неизбежно влечёт за собой корректировку властных отношений между участниками протокола, особенно при появлении возможности централизации в других местах. Как отмечено в [Schneider2], децентрализация «выглядит как риторическая стратегия, направляющая внимание на одни аспекты предлагаемого социального порядка и отвлекающая от других», поэтому «мы не можем воспринимать технологию как замену серьёзному отношению к социальным, культурным и политическим вопросам». Или более прямо, «без наличия механизмов управления узлы могут вступать в сговор, люди могут обманывать друг друга, рынки могут фальсифицироваться, а вход на рынок или выход с него могут быть связаны со значительными расходами» [Bodo]. Например, хотя криптовалюты на основе цепочек блоков (blockchain) призваны решить проблему централизации, присущую имеющимся валютам, техническими средствами, многие из них демонстрируют значительную концентрацию власти на основе голосования/майнинга, распределения средств и разнообразия баз кодов [Makarov]. Чрезмерная зависимость от технических мер также открывает возможности для скрытых неформальных властных структур, с которыми связаны свои риски, включая централизацию [Freeman].

В целом децентрализация функций требует значительных усилий, по сути является политическим процессом т связана со значительной неопределённостью в части результатов. Если рассматривать децентрализацию как социальную цель (в том смысле, который этот термин имеет в не связанном с компьютерами контексте), простая перестановка технических функций может привести к разочарованию. «Распределенная сеть не создаёт автоматически уравнительный, равноправный или просто социальный, экономический, политический ландшафт» [Bodo].

3.1. Стратегии децентрализации

В этом параграфе рассматриваются некоторые распространённые стратегии, применяемые для децентрализации функций Internet, и обсуждаются их ограничения.

3.1.1. Объединение

Разработчики протоколов часто пытаются решить проблему централизации путём объединения (федерации), т. е. функции разрабатываются так, чтобы использовались независимые экземпляры, поддерживающие связность и взаимодействие для предоставления одной целостной услуги. Федерация обещает дать пользователям возможность выбирать экземпляр, с которым они связаны, и заменять один экземпляр другим для снижения расходов на переключение. Однако объединения, самого по себе, недостаточно для предотвращения или смягчения централизации функции, поскольку нетехнические факторы могут вызвать необходимость использования централизованного решения.

Например, набор протоколов электронной почты должен маршрутизировать сообщения к пользователю, даже если тот меняет местоположение в сети или отключается на долгое время. Для решения этой задачи протокол SMTP [RFC5321] определяет особую роль для маршрутизации пользовательских сообщений - агент передачи сообщений (Message Transfer Agent или MTA). Позволяя любому развернуть MTA и определяя правила соединений между агентами, протокол избегает необходимости использования в этой роли центрального сервера. Пользователь может (и часто делает это) передать функции доставки кому-либо или запустить свой агент MTA.

Использование своего MTA со временем стало более обременительным отчасти из-за усложнения механизмов борьбы с нежелательной коммерческой почтой (спамом). Эти затраты стимулировали передачу функций MTA сторонним организациям, имеющим соответствующий опыт и ресурсы, что способствовало централизации рынка [Holzbauer]. Кроме того, меры, применяемые MTA для выявления нежелательной коммерческой почты, часто зависят от конкретного сайта. Поскольку крупные MTA обрабатывают гораздо больше адресов, возникает дисбаланс возможностей по сравнению с более мелкими агентами. Если крупный MTA сочтёт нежелательной почту от более мелкого, это существенно повлияет на способность того функционировать и возможность обратиться за помощью.

Расширяемый протокол обмена сообщениями и присутствия (Extensible Messaging and Presence Protocol или XMPP) [RFC6120] - это протокол общения (чат), который показывает ещё одну проблему федерации - добровольный характер технических стандартов. Как и электронная почта, XMPP использует объединение для облегчения встречи пользователей из разных систем, если они разрешают это. Хотя некоторые системы XMPP действительно поддерживают федеративный обмен сообщениями (т. е., человек, использующий службу A может общаться с пользователем службы B), многие из крупных систем не делают этого. Поскольку объединение является добровольным, некоторые операторы вынуждают клиентов пользоваться лишь одной службой, намеренно лишая их возможностей глобального взаимодействия.

Приведённые примеры показывают, что объединение не может гарантировать результат, хотя и создаёт условия для децентрализации функций.

3.1.2. Распределённое согласие

Технологии распределённого согласия (консенсуса), такие как блокчейн, всё чаще рассматриваются как решение проблемы централизации. Полный обзор этой быстро изменяющейся области выходит за рамки этого документа, но здесь приведено некое обобщение свойств.

Эти методы обычно гарантируют надлежащее выполнение функции с использованием криптографических методов (зачастую возможно лишь добавление в реестр транзакций). Они пытаются избежать централизации, распределяя выполнение функции между участниками протокола (иногда из большого пула). Обычно участники неизвестны и им нельзя доверять, а назначение узлу конкретной задачи для обработки невозможно предсказать или контролировать.

Sybil-атаки (одна или группа сторон дёшево создают достаточное для принятия согласия число участников) являются серьёзной проблемой таких протоколов, поскольку они ведут к концентрации власти в руках атакующего. Поэтому поощряется разнообразие в пулах участников с использованием косвенных методов, таких как доказательства работы (каждый участник должен показать значительное потребление ресурсов) или ставки (каждый участник имеет некий иной стимул для корректного выполнения работы).

Хотя эти меры могут быть эффективными для децентрализации работы функции, другие аспекты её предоставления могут быть централизованы (например, управление устройством, создание общих реализаций, документирование протоколов передачи). Необходимость координации является путём к централизации, даже если работа функции остаётся децентрализованной. Например «слияние» (merge) Ethereum показало, что блокчейн может решать экологические проблемы, но лишь при условии координированных усилий сообщества и правительства - координация, казавшаяся большинству безвредной, на деле была централизованной [ETHEREUM].

Кроме того, протокол или приложение с множеством функций может использовать распределённое согласие для некоторых функций, оставаясь централизованным в остальном по причине невозможности децентрализации других функций (чаще всего rendezvous и глобальное именование, см. параграф 2.2) или потому, что разработчик решил не делать этого из-за сопутствующих затрат и упущенных возможностей.

Эти возможные недостатки не исключают применения технологий распределенного согласия в каждом случае, но следует остерегаться некритического рассмотрения этих технологий как способа избежать или смягчить централизацию. Слишком часто использование распределенного согласия воспринимается как децентрализация всех частей проекта.

3.1.3. Оперативное управление

Объединение и распределённое согласие могут создавать условия для предоставления функции несколькими провайдерами, но не могут этого гарантировать. Однако когда поставщикам услуги требуется доступ к ресурсу или кооперация с другими, это узкое место может, само по себе, применяться для воздействия на поведение провайдера, включая противодействие централизации. В таких условиях для получения желаемого результата нужна та или иная форма управления этим узким местом. Зачастую это обеспечивается путём создания многостороннего органа, который представляет собой учреждение, включающее представителей разных сторон, влияющих на работу системы (заинтересованные стороны - stakeholder), в попытке обеспечить принятие обоснованных, легитимных и полномочных решений. Хорошо изученным примером такого метода является управление пространством имён DNS, которое раскрывает централизацию как «единый корень доверия» [Moura]. Этот источник доверия контролируется Корпорацией Internet по назначению имён и номеров (Internet Corporation for Assigned Names and Numbers или ICANN) <https://www.icann.org/resources/pages/governance/governance-en> - глобальным многосторонним органом, где представлены конечные пользователи, правительства, операторы и др.

Другим примером является управление моделью доверия в Web, реализуемое web-браузерами как полагающимися на доверие сторонами, у которых есть серьёзные стимулы для защиты приватности и безопасности пользователей, и CA в качестве привязки доверия, у которой есть серьёзные основания для включения в хранилище доверия браузера. Для продвижения операционных требований и требований безопасности, необходимых для обеспечения желаемых свойств был организован Форум CA/Browser <https://cabforum.org> в качестве надзорного органа, в котором участвуют обе стороны как заинтересованные лица.

Приведённые примеры примечательны тем, что механизм управления не задан напрямую в документации протокола, а накладывается оперативно, но так, чтобы использовались возможности протокола, способные ввести управление. Такое управление подходит лишь для сильно ограниченных функций, как в приведённых примерах. Даже в таких случаях создание и функционирование механизма управления не является тривиальной задачей, а его легитимность трудно обосновать и поддерживать (см., например, [Palladino]). Такой механизм по своей природе уязвим для захвата заинтересованными сторонами.

4. Что могут сделать стандарты Internet?

С учётом ограничений методов децентрализации, таких как объединение и распределенное согласие, добровольного соблюдения стандартов и мощных сил, которые могут способствовать централизации, резонно спросить, что могут сделать органы стандартизации, подобные IETF, чтобы приспособить полезную централизацию, избегая связанного с ней вреда и признавая, что само разграничение является по сути политическим решением. В последующих параграфах предложено несколько конкретных, значимых действий, которые могут предпринять органы стандартизации.

4.1. Повышение легитимности

Технические стандарты имеют лишь ограниченные возможности влияния на централизацию Internet, а правовые (регулирование, законодательство, прецедентное право) более перспективны в этом смысле и активно рассматриваются и внедряются в разных юрисдикциях. Однако регулирование Internet без чёткого понимания его влияния на архитектуру, основанного на технической точке зрения, связано с рисками. Такую точку зрения можно и следует предоставлять сообществу стандартизации Internet. Для этого соответствующие стороны (например, антимонопольные органы) должны считать легитимными организации сообщества. Если IETF будет восприниматься как организация, представляющая большие технологические компании или контролируемая ими, возможности воздействовать на решения, влияющие на Internet, существенно сокращаются. IETF уже имеет свойства, которые, возможно, обеспечивают достаточную легитимность. Примерами таких свойств являются открытое участие и представительство отдельных лиц, а не компаний, что повышает легитимность на входе, чётко заданный процесс с несколькими уровнями апелляций и прозрачностью, что повышает легитимность результатов, и долгая история разработки стандартов Internet, которая, пожалуй, лучше всего показывает легитимность IETF - результаты работы.

Однако также широко известно, что значительные расходы (не только финансовые), связанные с участием в работе IETF, ведут к тенденции отдавать предпочтение более крупным компаниям. Кроме того, специализированный технический характер работы создаёт препятствия для работы нетехнических заинтересованных сторон. Эти факторы могут снижать легитимность решений IETF, по крайней мере, для некоторых людей.

Работа по устранению этих недостатков продолжается, см., например, [RFC8890]. В целом, укрепление легитимности организации следует считать постоянной работой.

При участии во внешних работах, сообществу IETF (особенно руководству) следует помнить, что мнение организации наиболее авторитетно, когда оно сосредоточено на техническом и архитектурном влиянии.

4.2. Обсуждение централизации

Вопросы централизации и децентрализации все чаще поднимаются в ходе обсуждения технических стандартов. Любое заявление нужно оценивать критически. Как обсуждалось в разделе 2, не всякая централизация автоматически вредна. В соответствии с разделом 3, методы децентрализации не устраняют автоматически всякий вред централизации и могут вносить свои риски.

Однако участники разработки стандартов редко обладают достаточным опытом или сведениями для полной оценки таких утверждений, поскольку они включают не только технические факторы, но и экономические, социальные, коммерческие и юридические аспекты. Например, экономия от широкого распространения может привести к концентрации из-за связанной с этим эффективности [Demsetz], поэтому для оценки целесообразности такой концентрации нужен детальный экономический анализ, который не входит в сферу компетенции технических органов стандартизации. Кроме того, претензии на централизацию могут иметь и другие мотивы, например, они могут служить борьбе за власть между участниками с конкурирующими интересами, а также для блокирования участникам рынка и (что может быть важнее) пользователям возможности воспользоваться преимуществами стандартизации. Поэтому такие подходы, как требование включать в документы раздел «Вопросы централизации», публикация обзоров по централизации или выделение значительных ресурсов на поиск централизации в протоколах вряд ли улучшат Internet.

Отказ от стандартизации протокола по причине отсутствия активного предотвращения всех форм централизации игнорирует очень ограниченные возможности работ по созданию стандартов. Почти все имеющиеся протоколы Internet, включая IP, TCP, HTTP и DNS, не могут предотвратить централизацию применяющих эти протоколы приложений. Хотя одобрение проектов стандартов [RFC2026] не лишено ценности, простой отказ от него не помешает централизации.

Таким образом, обсуждение следует делать целенаправленным и ограниченным, а предложениям по децентрализации следует быть подробными, чтобы можно было полностью оценить их влияние. В [Schneider1] рекомендуется предлагающим децентрализацию быть «очень чёткими в плане указания конкретных свойств системы, которые предлагается децентрализовать» и предлагается продуманно применять такие инструменты, как разделение власти и подотчётность из «старой институциональной либеральной политической теории».

При оценке заявлений о децентрализованности конкретного предложения следует изучить контекст этих заявлений на предмет предпосылок, допущений и упущений. В [Bacchi] предложена схема критического опроса, которую можно приспособить к обсуждениям, связанным с централизацией.

1. Какова природа централизации, представляющейся проблематично?
2. Каковы глубинные предпосылки и допущения (концептуальная логика) лежат в основе представления «проблемы»?
3. Как возникло это представление проблемы?
4. Что остаётся избавленным от проблем в этом представлении? О чем умалчивается? Можно ли концептуализировать «проблему» иначе?
5. Какие последствия влечёт это представление «проблемы»?
6. Как и где это представление «проблемы» создавалось, распространялось и защищалось? Как оно было и/или может быть разрушено или заменено?

4.3. Целевые фирменные функции

Функции, которые широко распространены, но не имеют достаточной функциональной совместимости, созрели для стандартизации. Нацеливание на известные фирменные функции (например, чат) вполне уместно, так же как уместны незначительные усилия по улучшению функциональной совместимости и переносимости конкретных функций, которые часто применяются для привязки пользователей к платформе, например, формат списка контактов в социальной сети.

Основным возражением против такого подхода является его добровольное принятие - здесь нет «полиции стандартов» которая требовала бы от всех их применения или вынуждала к правильной реализации. Например, спецификации вроде [ACTIVITYSTREAMS] были доступны в течение некоторого времени, но не применялись на федеративной основе провайдерами коммерческих социальных сетей.

Это возражение игнорирует факт необязательности соблюдения стандартов и обязательности соответствия правовому регулированию. Законодательные требования к функциональной совместимости все чаще предлагаются регуляторами в качестве средства для решения проблем конкуренции (см., например, [DMA]). Это стремление к регулированию предоставляет новым спецификациям возможность децентрализации функций, подкреплённой правовым требованием, в сочетании с меняющимися нормами и связанными с этим рыночными силами [Lessig].

Такая возможность сопряжена с риском, если правовое регулирование противоречит архитектуре Internet. Создание стандартов, работающих совместно с правовым регулированием, сопряжено с возможными ловушками и требует новых и улучшенных возможностей (особенно взаимодействия), а также значительных усилий. Если техническое сообщество не предпримет таких усилий, регуляторы вполне могут обратиться к другим источникам разработки спецификаций функциональной совместимости.

4.4. Возможность переключения

Способность переключаться между разными поставщиками функций является основным механизмом контроля централизации. Если пользователи неспособны переключаться, они не смогут осуществить свой выбор или полностью реализовать значимость своих усилий, поскольку, например, «обучение работе с продукцией производителя требует времени и навык не может быть полностью перенесён на работу с продукцией конкурента, если нет должной стандартизации» [FarrellJ]. Поэтому явной целью стандартов должно быть облегчение для пользователей возможности перехода от одной реализации определения или обеспечения функций к другой.

Одним из необходимых условий переключения является наличие альтернативы, требуется широта и разнообразие реализаций и внедрения. Например, при единственной реализации протокола использующие его приложения будут уязвимы в части контроля за их действиями. Даже проекты с открытым кодом могут создавать такие проблемы, если имеются факторы, осложняющие создание ветвей проекта (например, стоимость поддержки ветви). В параграфе 2.1 [RFC5218] рассмотрены некоторые факторы, способствующие разнообразию реализаций при разработке протоколов.

Стоимость перехода пользователей на другую реализацию или развёртывание является ещё одним фактором, который следует учитывать. Это учитывает расход времени и ресурсов, требуемый опыт и координацию, потерю функциональности, а также усилия, требуемые для работы с другим провайдером или реализацией, при этом подразумевается, что стандарт должен быть достаточно полным и точным, чтобы замена стала возможной.

Цели достижения полноты и разнообразия иногда противоречат друг другу. Если стандарт становится чрезвычайно сложным, это может стать препятствием для разнообразия реализаций, поскольку стоимость полной реализации будет слишком высокой (вспомним web-браузеры). С другой стороны, слишком простая спецификация может не обеспечить простого переключения, особенно если для полноты нужны нестандартные (proprietary) расширения (см. параграф 4.7).

Одним из возражений против протоколов, допускающих простое переключение, является снижение стимулов для их реализации коммерческими производителями (поставщиками). Хотя полностью коммерциализированный протокол может не позволить реализациям различаться, у них остаётся возможность специализации и совершенствования с других частях цепочки добавления стоимости [Christensen]. Своевременная работа по стандартизации служит сосредоточению интересов компаний на применении открытых технологий, а не на их замене.

4.5. Управление передачей полномочий

Пользователи некоторых функций могут получить дополнительные преимущества, обеспечиваемые третьей стороной.

Efficiency - эффективность

Эффективность многих функций Internet может повышаться при выполнении в большем масштабе. Например, сеть доставки содержимого может предоставлять услуги за часть финансовых и экологических затрат, которые иначе пришлось бы нести тому, кто сам обслуживает содержимое, поскольку его масштабы меньше. Аналогичным образом, двухсторонняя торговая платформа может повышать эффективность по сравнению с обычной торговлей продавец-покупатель [Spulber].

Simplicity - простота

Полное исключение посредников при взаимодействии может перенести издержки функций на конечные точки, что может повысить когнитивную нагрузку на пользователей. Сравните, например, платформы коммерческих социальных сетей с усилиями по самостоятельному размещению.

Specialization - специализация

Консолидация функций в нескольких руках может улучшать результаты за счёт специализации. Например, службы, управляемые профессиональными администраторами, зачастую обеспечивают более высоки уровень безопасности и доступности.

Privacy - приватность

Для некоторых функций приватность пользователей можно повысить за счёт консолидации действий, позволяющей предотвратить распознавание поведения отдельных людей [Chaum]. Добавление третьей стороны может также установить функциональные границы, например, избавить пользователей от необходимости доверять потенциально вредоносным конечным точкам, как это случается в так называемых «забывчивых» (oblivious) протоколах (например, [RFC9230]), которые позволяют пользователям скрыть своё отождествление от сервиса, сохраняя доступ к нему.

Однако если эта новая сторона сделает своё участие «липким» (sticky), например, используя своё положение в сети, чтобы требовать использования посредника, применяя свой доступ к данным или воспользовавшись сложностью переключения на другого провайдера функции, это ведёт к риску централизации. Чаще всего третья сторона добавляется к функциям в форме посредника или назначенного агента. Разработка функций с продуманными ограничениями для таких ролей может предотвратить хотя бы вопиющие злоупотребления властью.

Для случаев вовлечения в функцию третьей стороны оказались полезными два правила. Во-первых, третьей стороне следует вмешиваться во взаимодействие, когда хотя бы одна из двух сторон предпринимает позитивные действия для этого. Во-вторых, третьей стороне следует быть способной наблюдать или контролировать взаимодействия, ограничиваясь лишь тем, что необходимо для выполнения предусмотренной функции. Например, ранние реализации HTTP позволяли посредникам вмешиваться в сеть без знания конечных точек и эти посредники могли по умолчанию видеть и изменять всё содержимое трафика, даже будучи предназначенными для выполнения лишь базовых функций, таких как кэширование. В результате введения HTTPS и метода CONNECT (см. параграф 9.3.6 в [HTTP]) в сочетании с усилиями по их внедрению посредники сейчас должны явно указываться конечной точкой и имеют доступ лишь к базовым маршрутным сведениям. Дополнительные сведения о протокольном посредничестве приведены в [THOMSON-TMI].

Термин «посредник» часто применяется (особенно в правовом и нормативном контексте) в более широком смысле, нежели для протоколов. Например, web-сайт аукциона, посредничающий между продавцами и покупателями, является посредником, хотя формально не выполняет функций посредника HTTP (см. параграф 3.7 в [HTTP]). Разработчики протоколов могут решить проблему централизации, связанную с такого рода посредничеством, путём стандартизации функции, а не ограничения возможностей базовых протоколов (см. параграф 4.3).

4.6. Установка границ

Большинство протоколов и приложений Internet зависят от других функций «нижележащего уровня» и их реализаций. Свойства, развёртывание и функционирование этих зависимостей могут вносить риск централизации для работающих на их основе функций и приложений. Например, протоколам приложений нужна для работы сеть, поэтому поставщик сетевых услуг имеет определённую власть над коммуникациями. Он может заблокировать или замедлить доступ, изменить содержимое соответствующего сервиса по финансовым, политическим, операционным или криминальным причинам, создавая препятствия (или даже лишая возможности) для использования конкретного поставщика функции. Выборочно препятствуя использованию одних услуг (но не других), сетевое вмешательство можно организовать так, что оно будет (намеренно или ненамеренно) принуждать к использованию других услуг.

Такие методы, как шифрование, могут препятствовать централизации, устанавливая границы. Когда число сторон, имеющих доступ к содержимому взаимодействия, ограничено, другим сторонам, которые обрабатывают коммуникации, но не являются их частью, можно запретить вмешиваться в содержимое и наблюдать его. Хотя эти стороны по-прежнему могут препятствовать взаимодействию, шифрование затруднит распознавание цели среди трафика других пользователей.

4.7. Осторожность при расширении

Способность Internet к развитию имеет решающее значение, позволяя соответствовать новым требованиям и адаптироваться к новым условиям без «дня флага» для обновления реализаций. Обычно функции поддерживают развитие путём определения интерфейсов расширения, которые позволяют добавлять или изменять функции с течением времени обеспечивающим функциональную совместимость способом. Однако эти интерфейсы могут быть использованы сильной стороной, если они могут менять цель для обеспечения значимой совместимости путём добавления своих (proprietary) расширений к стандарту. Это особенно верно в случаях, когда сам базовый стандарт не обеспечивает достаточной полезности. Например, чрезвычайная гибкость SOAP [SOAP] и неспособность обеспечить самостоятельную ценность позволяет производителям требовать использования определённых расширений, отдавая предпочтение тем, кто сильней на рынке.

Поэтому усилия по стандартизации должны быть нацелены на обеспечение конкретной полезности для большинства пользователей в опубликованном виде, а не на создание основы, где функциональная совместимость не доступна сразу. Функциям Internet не следует делать расширяемым каждый аспект работы и между модулями следует задавать границы, которые позволят развиваться и разрешать (но не гарантировать) децентрализацию. Продуманные

интерфейсы не только позволят развиваться, но и будут способствовать усилиям по децентрализации. Структурные границы между субмодулями функции, а также между смежными функциями, обеспечивают точки соприкосновения для функциональной совместимости и возможность смены провайдеров. В частности, стабильные и чётко определённые интерфейсы дают возможность использовать разных поставщиков функции. Когда эти интерфейсы являются открытыми стандартами, контроль изменений переходит к техническому сообществу, а не остаётся в руках компаний, что дополнительно повышает стабильность и способствует (без гарантий) децентрализации.

4.8. Использование того, что работает

Когда централизация намеренно разрешена для функции Internet, разработчики протоколов часто пытаются смягчить связанные с ней риски, используя технические меры, такие как объединение (параграф 3.1.1) и структуры оперативного управления (параграф 3.1.3). Протоколы, успешно справляющиеся с такой задачей, часто применяются неоднократно, чтобы избежать значительных трат и рисков, связанных с повторной реализацией этих мер. Например, если протоколу нужна скоординированная глобальная функция именования, включение DNS обычно предпочтительней создания новой системы.

5. Продолжение работы

В этом документе утверждается, что, несмотря на малые возможности органов стандартизации эффективно контролировать и предотвращать централизацию Internet через разработку протоколов, всё же имеются конкретные и полезные действия, которые они могут предпринять для улучшения Internet. Эти действия могут быть разработаны и расширены в будущих работах, однако несомненно, что можно сделать ещё больше. Можно выявить и изучить новые методы децентрализации, документировать то, что стало известно из взаимодействия с другими, более эффективными регуляторами в этой области.

Имеются предложения создать руководство или контрольный список для работы с централизацией. Поскольку централизация очень разнообразна в проявлениях и сильно зависит от контекста, лучшим решением может оказаться её предотвращение в ограниченных областях, например, для конкретного типа функций или определённого уровня.

Природа централизации и, в частности, её причины также заслуживают дальнейшего изучения. Хотя имеется много комментариев о таких факторах, как влияние сети и стоимость переключения, другие факторы, такие как поведенческие, когнитивные, социальные аспекты, изучены пока достаточно слабо, однако ситуация меняется (см., например, [Fletcher]).

6. Вопросы безопасности

Этот документ не оказывает прямого влияния на безопасность протоколов Internet. Тем не менее, отказ от учёта централизации может вызывать множество проблем безопасности, предварительное обсуждение которых приведено в параграфе 2.1.

7. Взаимодействие с IANA

Этот документ не требует действий IANA.

8. Литература

[Abrahamson] Abrahamson, Z., "Essential Data", Yale Law Journal, Vol. 124, No. 3, December 2014, <https://www.yalelawjournal.org/comment/essential-data>.

[ACTIVITYSTREAMS] Prodromou, E., Ed. and J. Snell, Ed., "Activity Streams 2.0", W3C Recommendation, 23 May 2017, <https://www.w3.org/TR/2017/REC-activitystreams-core-20170523/>. Latest version available at <https://www.w3.org/TR/ activitystreams-core/>.

[Aligia] Aligia, P. and V. Tarko, "Polycentricity: From Polanyi to Ostrom, and Beyond", Governance: An International Journal of Policy, Administration, and Institutions, Vol. 25, No. 2, p. 237, DOI 10.1111/j.1468-0491.2011.01550.x, April 2012, <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-0491.2011.01550.x>.

[Bacchi] Bacchi, C., "Introducing the 'What's the Problem Represented to be?' approach", Chapter 2, Engaging with Carol Bacchi, 2012, <https://library.oapen.org/bitstream/handle/20.500.12657/33181/560097.pdf?sequence=1#page=34>.

[Baran] Baran, P., "On Distributed Communications: Introduction to Distributed Communications Networks", DOI 10.7249/RM3420, 1964, <https://www.rand.org/pubs/research_memoranda/RM3420.html>.

[BCP95] Alvestrand, H., "A Mission Statement for the IETF", BCP 95, RFC 3935, October 2004. <https://www.rfc-editor.org/info/bcp95>

[Bodo] Bodó, B., Brekke, J. K., and J.-H. Hoepman, "Decentralization: a multidisciplinary perspective", Internet Policy Review, Vol. 10, No. 2, DOI 10.14763/2021.2.1563, June 2021, <https://policyreview.info/concepts/decentralisation>.

[Chaum] Chaum, D., "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of the ACM, Vol. 24, No. 2, DOI 10.1145/358549.358563, February 1981, <https://dl.acm.org/doi/10.1145/358549.358563>.

[Christensen] Christensen, C., "The Law of Conservation of Attractive Profits", Harvard Business Review, "Breakthrough Ideas for 2004", February 2004.

[Demsetz] Demsetz, H., "Industry Structure, Market Rivalry, and Public Policy", Journal of Law and Economics, Vol. 16, No. 1, April 1973, <https://www.jstor.org/stable/724822>.

[DMA] The European Parliament and the Council of the European Union, "Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)", OJ L 265/1, 12.10.2022, September 2022, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>.

[Doctorow] Doctorow, C., "Adversarial Interoperability", October 2019, <https://www.eff.org/deeplinks/2019/10/adversarial-interoperability>.

[ETHEREUM] Ethereum, "The Merge", February 2023, <https://ethereum.org/en/roadmap/merge/>.

[FarrellH] Farrell, H. and A. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion", International Security, Vol. 44, No. 1, p. 42, DOI 10.1162/ISEC_a_00351, July 2019, <https://doi.org/10.1162/ISEC_a_00351>.

[FarrellJ] Farrell, J. and C. Shapiro, "Dynamic Competition with Switching Costs", UC Berkeley Department of Economics Working Paper 8865, DOI 10.2307/2555402, January 1988, <https://doi.org/10.2307/2555402>.

[Fletcher] Fletcher, A., "The Role of Behavioural Economics in Competition Policy", DOI 10.2139/ssrn.4389681, March 2023, <https://doi.org/10.2139/ssrn.4389681>.

[Freeman] Freeman, J., "The Tyranny of Structurelessness", Berkeley Journal of Sociology, Vol. 17, 1972, <https://www.jstor.org/stable/41035187>.

[Holzbauer] Holzbauer, F., Ullrich, J., Lindorfer, M., and T. Fiebig, "Not that Simple: Email Delivery in the 21st Century", July 2022, <https://www.usenix.org/system/files/atc22-holzbauer.pdf>.

[HTTP] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "HTTP Semantics", STD 97, RFC 9110, DOI 10.17487/RFC9110, June 2022, <https://www.rfc-editor.org/info/rfc9110>.

[Kashaf] Kashaf, A., Sekar, V., and Y. Agarwal, "Analyzing Third Party Service Dependencies in Modern Web Services: Have We Learned from the Mirai-Dyn Incident?", DOI 10.1145/3419394.3423664, October 2020, <https://dl.acm.org/doi/pdf/10.1145/3419394.3423664>.

[Komaitis] Komaitis, K., "Regulators Seem to Think That Facebook Is the Internet", August 2021, <https://slate.com/technology/2021/08/facebook-internet-regulation.html>.

[Lessig] Lessig, L., "The New Chicago School", Journal of Legal Studies, Vol. 27, DOI 10.1086/468039, June 1998, <https://www.journals.uchicago.edu/doi/10.1086/468039>.

[Madison] Madison, J., "The Structure of the Government Must Furnish the Proper Checks and Balances Between the Different Departments", The Federalist Papers, No. 51, February 1788.

[Makarov] Makarov, I. and A. Schoar, "Blockchain Analysis of the Bitcoin Market", National Bureau of Economic Research, Working Paper 29396, DOI 10.3386/w29396, October 2021, <https://www.nber.org/papers/w29396>.

[Marlinspike] Marlinspike, M., "Reflections: The ecosystem is moving", May 2016, <https://signal.org/blog/the-ecosystem-is-moving/>.

[Moura] Moura, G., Castro, S., Hardaker, W., Wullink, M., and C. Hesselman, "Clouding up the Internet: how centralized is DNS traffic becoming?", DOI 10.1145/3419394.3423625, October 2020, <https://dl.acm.org/doi/abs/10.1145/3419394.3423625>.

[Musiani] Musiani, F., "Alternative Technologies as Alternative Institutions: The Case of the Domain Name System", The Turn to Infrastructure in Internet Governance, DOI 10.1057/9781137483591_4, 2016, <https://link.springer.com/chapter/10.1057/9781137483591_4>.

[Palladino] Palladino, N. and M. Santaniello, "Legitimacy, Power, and Inequalities in the Multistakeholder Internet Governance", DOI 10.1007/978-3-030-56131-4, November 2020, <https://link.springer.com/book/10.1007/978-3-030-56131-4>.

[PHONE] Skrzycki, C. and J. Burgess, "Computer Failure Paralyzes Region's Phone Service", June 1991, <https://www.washingtonpost.com/archive/politics/1991/06/27/computer-failure-paralyzes-regions-phone-service/0db94ac7-89f0-446e-ba33-c126c751b251/>.

[RFC2026] Bradner, S., "The Internet Standards Process - Revision 3", BCP 9, RFC 2026, DOI 10.17487/RFC2026, October 1996, <https://www.rfc-editor.org/info/rfc2026>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC5218] Thaler, D. and B. Aboba, "What Makes for a Successful Protocol?", RFC 5218, DOI 10.17487/RFC5218, July 2008, <https://www.rfc-editor.org/info/rfc5218>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://www.rfc-editor.org/info/rfc5321>.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, DOI 10.17487/RFC6120, March 2011, <https://www.rfc-editor.org/info/rfc6120>.

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[RFC8890] Nottingham, M., "The Internet is for End Users", RFC 8890, DOI 10.17487/RFC8890, August 2020, <https://www.rfc-editor.org/info/rfc8890>.

[RFC9230] Kinnear, E., McManus, P., Pauly, T., Verma, T., and C.A. Wood, "Oblivious DNS over HTTPS", RFC 9230, DOI 10.17487/RFC9230, June 2022, <https://www.rfc-editor.org/info/rfc9230>.

[RFC9293] Eddy, W., Ed., "Transmission Control Protocol (TCP)", STD 7, RFC 9293, DOI 10.17487/RFC9293, August 2022, <https://www.rfc-editor.org/info/rfc9293>.

[Schneider1] Schneider, N., "What to do once you admit that decentralizing everything never seems to work", Hacker Noon, September 2019, <https://hackernoon.com/decentralizing-everything-never-seems-to-work-2bb0461bd168>.

[Schneider2] Schneider, N., "Decentralization: An Incomplete Ambition", Journal of Cultural Economy, Vol. 12, No. 4, DOI 10.31219/osf.io/m7wyj, April 2019, <https://osf.io/m7wyj/>.

[SOAP] Mitra, N., Ed. and Y. Lafon, Ed., "SOAP Version 1.2 Part 0: Primer (Second Edition)", W3C Recommendation, 27 April 2007, <https://www.w3.org/TR/2007/REC-soap12-part0-20070427/>. Latest version available at <https://www.w3.org/TR/soap12-part0/>.

[Spulber] Spulber, D., "Solving The Circular Conundrum: Communication and Coordination in Two-Sided Markets", Northwestern University Law Review, Vol. 104, No. 2, October 2009, <https://wwws.law.northwestern.edu/research-faculty/clbe/workingpapers/documents/spulber_circularconundrum.pdf>.

[THOMSON-TMI] Thomson, M., "Principles for the Involvement of Intermediaries in Internet Protocols", Work in Progress, Internet-Draft, draft-thomson-tmi-04, 8 September 2022, <https://datatracker.ietf.org/doc/html/draft-thomson-tmi-04>.

Благодарности

Этот документ родился из ранних обсуждений с Brian Trammell во время совместной работы в Совете по архитектуре Internet (Internet Architecture Board или IAB).

Особая благодарность Geoff Huston и Milton Mueller за продуманные и полезные рецензии.

Спасибо Jari Arkko, Kristin Berdan, Richard Clayton, Cory Doctorow, Christian Huitema, Eliot Lear, John Levine, Tommy Pauly, Martin Thomson за их комментарии и предложения. Ценные обсуждения и отклики предоставили список рассылки arch-discuss@ietf.org и исследовательская группа Decentralized Internet Infrastructure.

При подготовке документа не использовались большие языковые модели.

Адрес автора

Mark Nottingham
Prahran
Australia
Email: mnot@mnot.net
URI: https://www.mnot.net/

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru