И. Белоусов Элиот Крон
А. Пискунов В. Попов С. Симановский

WEB 3.0.

ЧАСТЬ I.
НАСТОЯЩЕЕ ВЧЕРАШНЕГО ЗАВТРА

И. Белоусов
С. Симановский
В. Попов
Э. Крон
А. Пискунов

Web 3.0. Часть I. Настоящее вчерашнего завтра

http://www.litres.ru/pages/biblio_book/?art=51616788
ISBN 9785449842503

Аннотация

Это первая часть первой русскоязычной книги о Web 3.0. Не только о том, каким будет, но и о том, каким видится разным людям: от разработчиков до предпринимателей. Кроме того, это совместный труд сразу нескольких специалистов, что делает прочтение полезным для тех, кто с технологиями и на ты, и на вы.

Содержание

Web 3.0.
Часть I. Настоящее вчерашнего завтра

Посвящается Д. Ассанжу и всем, кто пострадал от рук виновных

Авторы: Белоусов И., Крон Э., Пискунов А., Попов В., Симановский С.

ISBN 978-5-4498-4250-3 (т. 1)
ISBN 978-5-4498-4251-0
Создано в интеллектуальной издательской системе Ridero

Общие вводные

Компания AOL когда-то считала, что массовое создание сайтов возможно только после «прыжка веры». Как видим, он таки случился…

Данный труд является совместным сразу для нескольких криптоэнтузиастов: И. Белоусова (The Power), А. Пискунова (Viz), В. Попова (Synergis & Menaskop), Э. Крона (Псевдоним), С. Симановского (Blocksult). Написана книга *для всех*, но в первую очередь для тех, кто хочет создавать по-настоящему инновационный бизнес (предпринимателям), а равно и тем, кто желает помогать его развивать (архитекторам систем, разработчикам и так далее). В начале представлены позиции относительного того, а что же есть Web 3.0 (**далее – W3**), чем так примечателен и как именно его можно использовать. Затем следуют разделы по разным направлениям. Пожалуй, самым важным для нас, авторов, является то, что книга – первая[1] в своём роде, а значит, с её помощью можем прочувствовать пульс рынка: кому именно нужен тот стек технологий, который заложен в Web 3.0? Кто готов вкладывать свои силы, время, деньги, чтобы он эволюционировал? Какие кейсы получат наибольшее развитие се-

[1] Полноценная о Web 3.0 на русском языке (прим. В.П.).

годня, а какие – в ближайшем будущем? Как бы там ни было, стоит помнить, что блокчейн, пришедший к нам более десяти лет назад, уже породил множество альтернативных инструментов, которые на полную мощность могут применяться только в парадигме Web 3.0, но и это – не всё: эволюция p2p – прямое свидетельство необходимости следующего шага. Если нравится участвовать в создании чего-то новаторского – обязательно свяжитесь с выпускающим редактором, найдя в одной из социальных сетей ник **Menaskop**, или даже по почте – menaskop@gmail.com.

А пока – приятного чтения и важных выводов: встретимся в заключении!

Как правильно читать книгу?

Поскольку авторов несколько, каждый из них по-своему уникален, а значит – субъективен, книгу можно читать с любой части: для начинающих рекомендуем приложение №1, а затем – введение и далее, для опытных, – любую главу.

Официальное определение

Как ни странно, но оно есть (и даже Wiki на этом настаивает): по вот этой ссылке. Процитируем: «Некоторые люди спрашивали меня (*Д. Калаканиса – прим. авт.*) о чётком определении термина Web 3.0. Web 3.0 определяется как создание высококачественного контента и услуг, производимых талантливыми людьми с использованием технологии Web 2.0[2] в качестве платформы, предоставляющей подобную возможность. Сервисы Web 2.0 в настоящее время являются коммодитизированной платформой[3], а не конечным продуктом. Мир, где социальная сеть, вики или сервис социальных закладок могут быть построены бесплатно и в одно мгновение, есть, что дальше?

Сервисы Web 2.0, такие как digg и YouTube, превращаются в сервисы Web 3.0 с дополнительным уровнем индивидуального мастерства и сосредоточенности. В качестве примера приведу funnyordie.com, сервис, который использует все стандартные наборы функций Web 2.0, такие как синдикация и социальные сети, добавляя к ним слои особого таланта и доверия…

Web 3.0 – возвращение к тому, что было великим в средствах массовой информации и технологии до Web 2.0: при-

[2] На мой взгляд – в этом он сильно ошибался (прим. В.П.).

[3] То есть ориентированной на массовое потребление (прим. В.П.).

знание таланта и опыта, право собственности на контент и справедливость (повсюду). Пришло время развиваться».

Есть и другая позиция на сей счёт, высказанная Н. Спиваком[4] также в 2007 году (подробней об этой дискуссии можно прочесть в приложении №3): «Джейсон только что написал в блоге об официальном определении Web 3.0 – в его случае он определяет его как лучший контент, созданный с использованием технологий Web 2.0. Было много ответов на сей счёт, но так как я один из основных соавторов страницы Википедии по термину Web 3.0, то подумал, что должен бросить и забить свою шайбу в эти ворота.

Web 3.0, на мой взгляд, лучше всего определить как третье десятилетие[5] Сети (2009—2019), в течение которого несколько ключевых технологий будут широко использоваться. Главными среди них будут RDF и технологии развивающейся Семантической паутины. Хотя Web 3.0 не является синонимом Семантической паутины (в этот период произойдёт ещё несколько *важных* технологических сдвигов), он будет в значительной степени характеризоваться семантикой в целом.

Web 3.0 – эра, в которой модернизируем бэкенд Сети по-

---

[4] Который опубликован по известному адресу – https://novaspivack.typepad.com/nova_spivacks_weblog/2007/10/web-30–the-a.html.

[5] Интересно, что в ответе Д. О'Рейли и в Интернете часто приводится другой период – с 2010 по 2020 годы (прим. В.П.), потому как именно и сам автор перешёл на округление до этого периода: 1990—2000, 2000—2010, 2010—2020 и т. д.

сле десятилетия фокусировки на фронтенде (Web 2.0 в основном был посвящён AJAX, тегам и другим инновациям фронтенда для пользователей). Web 3.0 уже начинает появляться в таких стартапах, как Radar Networks (и наш продукт – Twine), но на самом деле станет мейнстримом[6] примерно в 2009 году.

Почему определение Web 3.0 лучше, чем любое другое возможное определение этого термина? Во-первых, это дефиниция, которая не может быть легко экспроприирована[7] любой компанией или частным лицом под какую-либо конкретную технологию или продукт. Это совершенно однозначное определение и относится к определённому периоду времени и всему, что происходит в веб-технологиях и бизнесе в течение этого периода. Это положит конец дебатам о том, что означает сей термин, и перенесёт его в область полезного обсуждения, а именно: какие технологии и тенденции *на самом деле* станут важными в грядущем десятилетии Сети?».

Что ж, последние 10—12 лет подтвердили верность второго и относительную ошибочность первого подхода, но произведение наше как раз о том, что не всё так просто…

---

[6] Так оно и вышло: Белая книга Биткоина написана в 2008 году, а первая транзакция совершена именно в 2009-м, как и намайнен первый блок.

[7] В оригинале использовано понятие co-opted (кооптация), которое дословно можно перевести как смыкание или же введение в состав чего-либо без дополнительного согласования, но остановился, как и везде далее, на передаче смысла, а не побуквенном переводе (прим. В.П.).

глоссарий сокращений

ГСР/СГР – глобальная система репутации / система глобальной репутации

ДРС – децентрализованные и/или распределённые системы

ПО – программное обеспечение

SaO – субъект и объект (внутри ДРС)

W3 – Web 3.0

Дисклеймеры

Поскольку книга написана несколькими авторами, а равно – подвержена была общей редактуре, то позиции одного из участников могут не совпадать с другими, а порой – коренным образом расходиться, но в этом и прелесть децентрализации: можно увидеть как можно больше разного. Пусть это не смущает.

Второе замечание заключается в том, что в книге (по крайней мере – в электронном варианте) множество ссылок: при первом прочтении их можно смело опустить, а при повторном и последующих – использовать в качестве ***справочника****. Иногда (в силу особенностей вёрстки) приходилось заменять ссылки русскоязычной Википедии на англоязычную: вы всегда можете сменить язык в нижнем левом углу на сайте wikipedia.org.*

Web 3.0: начала

От автора главы

«Web 3.0 – эра, в которую будем обновлять бэкенд сети после десятилетия фокуса на фронтенде».
Н. Спивак

Привет! Меня зовут Анатолий Пискунов[8], уже более пятнадцати лет изучаю интернет-технологии. Всё начиналось как хобби, переросло в небольшие проекты, эксперименты, изучение разных решений, десятки (если не сотни) прочитанных книг, профильное и самостоятельное изучение всего, что связано с Сетью. Верстал, программировал, администрировал, пробовал разные подходы, падал и (снова) вставал, устраивался на работу, менял компании, руководил разработкой сервисов, работал с тендерами, брался за разные, даже невозможные на первый взгляд проекты и завершал их. В 2016 году ушёл с работы и нырнул в блокчейн-сферу: целиком и надолго.

Думаю, у каждого блокчейн-энтузиаста своя специализация и свой спектр увлечений. И я не исключение: больше

[8] Помимо прочего Анатолий является одним из создателей VIZ.

всего интересует именно Интернет и новые возможности, которые привнесут в него системы распределённого реестра. Возможно, мой взгляд на Web 3.0 не покажется «стандартным», но, постарался донести и передать словами то, что вижу. Надеюсь, после прочтения почувствуешь «это», получишь заряд энергии и воодушевления (а может, и новые вопросы).

Буду рад отзывам и комментариям!

Введение к главе первой

«Нумерация Интернета?!
Что за глупости, Интернет есть Интернет!
Или всё же…»
Аноним

Предположу, что часть читателей застали эпоху dial-up-Интернета[9]. Что в то время было? Адресная строка и каталоги сайтов. Сайты на Народе (сервис бесплатного размещения от Яндекса), html-страницы, баннеры на дружественные ресурсы, которыми обменивались вручную, js-скрипты, которые использовались зачастую для эмуляции падающего снега, летающих за мышкой картинок, и тесты на одной странице. CGI-модули для гостевых книг и борьба с KOI8-R.

Переход от Web 1.0 к Web 2.0 был постепенным. Серверные скрипты на Perl сменялись PHP, автоматические механизмы регистрации, первые капчи, панели администрирования, модульные надстройки над форумами (привет, PHP-Nuke!). Хостинг-провайдеры конкурировали за пользователей, предлагая всё новые версии PHP и MySQL (позже стали внедрять cPanel). Flash-анимация, ActionScript и видеоигры

[9] Здесь и далее предпочитаем использовать слово Интернет, написанное с заглавной буквы, если речь идёт о всей сети в целом, поскольку часто будем говорить об альтернативах сегодняшним, пусть и наиболее глобальным, решениям (прим. В. П.).

в браузере.

Предлагаю оставить термин Web 2.0 для справочников и энциклопедий. Кто впервые публично произнёс термин, что в это вкладывал – всё в прошлом и не так важно. Интернет эволюционирует постоянно. Это происходит и сейчас. Мы – свидетели чуда. Так ли значимо, в каком году появился AJAX, когда родилась библиотека JQuery и прекратили обновлять страницу в почтовом сервисе для того, чтобы проверить, а пришли ли новые письма? Когда алгоритмы стали автоматически маркировать спам? Когда появилась технология потокового видео и YouTube? Когда люди стали переходить из ICQ в Jabber, а позже в Skype? Когда онлайн-созвон, чтобы совместно играть в MOBA, стал нормой?

Социальные сети создали точку сбора: формирование сообществ и групп перенесло живое общение в онлайн. Эволюция – процесс постепенный. Какие-то инновации потерпели крах, какие-то стали естественным продолжением нас. Теперь у каждого есть смартфон с возможностью осуществления социального взаимодействия дабл-тапом по фотографии в Инстаграме. Слои социума поделены между глобальными соцсетями. Для трудоголиков и профессионалов есть LinkedIn от Microsoft. Для старшего поколения – ламповые «Одноклассники» (которые мудро изменили позиционирование, переименовавшись в ОК). Для творческих натур и визуализаторов – Инстаграм. Для любителей читать суть – Твиттер (или TL; DR, который обходится модными картин-

ками с текстом или кликбейт-заголовками). Телевизор с пропагандой успешно заменён на YouTube, где сформированный пользователем круг подписок создаёт замкнутый мир по интересам.

WebSocket и WebAssembly прямо сейчас закладывают фундамент для следующей ступени развития. Адаптивная вёрстка уже необходимость: способ потреблять информацию изменился, и для основной массы выбор очевиден. Впереди – VR/AR-революция, и есть опасения, что человечество собственноручно откажется от реалистичного восприятия в угоду реалистичной картинке.

Исторически сложилась простая истина: инновации и технологии сталкиваются с испытаниями временем (Flash уже проиграл Canvas и HTML5), удобством (noSQL всё чаще замещают реляционные базы данных), адаптацией под настоящее (осознание вреда экологии от … – *острая* повестка для всего человечества). Выжившие камень за камнем выкладывают мозаику под названием Интернет[10]. И главное: мы – участники и свидетели процесса.

[10] А ещё точнее – Интернет 2.0, потому как альтернативных сетей должно быть как можно больше (прим. В. П.).

Что же такое Web 3.0?

Все сервисы или компании, которые применяют термин Web 3.0, добиваются ровно одного: привлечь внимание к своей технологии, заявить о себе как об инновации, которая займёт нужное и важное место в истории. Это одновременно и метка, и маркетинговый ход, и заявка на общественное внимание. Сколько людей в своё время обогатилось, вложив в пионеров[11] – Amazon, eBay, Facebook, Alphabet (в прошлом Google)? Они правильно разглядели тренды, потенциал продуктов и решений, которыми занимались те или иные компании. Думаю, уже закрадывается сомнение, что спустя несколько лет в справочнике появится запись: «Web3.0 – это… технологическое решение, которое использовало инновационную парадигму… и предоставило пользователям решение актуальной проблемы…». *Мы находимся в состоянии Web 3.0* Шрёдингера. Осознание, что Web 3.0 наступил, придёт тогда, когда придёт. Остаётся быть созидателями инноваций и движителями парадигм. Предлагаю рассмотреть существующие интерпретации новой главы Интернета от компаний и персон, готовых приложить усилия и имеющих смелость заявить о том, что именно они – часть этого нового.

[11] Но стоит помнить, что тех, кто обанкротился на пузыре доткомов, – значительно больше! (Прим. В. П.).

Интерпретации Web 3.0

С популяризацией криптовалют начал происходить концептуальный сдвиг в понимании экономики и ценности среди пользователей, обладающих достаточной технической грамотностью. Биткоин доказал свою жизнеспособность и состоятельность криптографических децентрализованных систем. Привлечение внимания общественности к цифровой ценности породило большую волну участников рынка, которые верят в развитие блокчейна (или, как стали называть эту технологию в научной среде, DLT[12]). Как итог – появились новые системы самого разного назначения. Не обошлось и без мошенников, рисующих красивые обёртки для сбора средств путём краудфандинга[13]. Но реальный новый сектор DLT уже невозможно остановить. Интеллектуальный вклад в развитие этой IT-находки раскрывает отрасли шаг за шагом.

Открытость, доказуемость действий, возможность независимого аудита и распределённость привели к смене парадигмы в умах сознательных людей. Именно люди стали пере-

[12] Всё же для меня (В. П.) DLT и blockchain – равнопорядковые, но разные явления.

[13] Не стоит преувеличивать их значение: отчёт-исследование ico с 2013 по 2018 гг. показал, что уровень скама в данной сфере не достигал и 20%, что значительно ниже, чем в отрасли банковского кредитования и в венчурном инвестировании.

носить концепцию нового мышления на привычные вещи. Биткоин сделал это в рамках финансового мира. Но остаётся столько[14] всего!

Приватность. Защита персональных данных. Право на тайну[15] личной переписки. Договоры и сделки без посредников (смарт-контракты).

Идея о том, что можно исключить посредника, начала поступательное движение на все элементы привычного Интернета. Энтузиасты и разработчики стали озираться по сторонам, выискивая бизнес-процессы, где есть посредники. Можно ли от них отказаться? Вот краткий список:

– Доменные имена? Есть продавец и посредники-реселлеры, которые по желанию левой пятки могут поднять цену или заблокировать домен по жалобе регуляторов. Можно отказаться от них и разработать собственные беспристрастные механизмы общего пространства[16] имён!

– Сертификационные центры (SSL)? Посредники есть! Браузеры[17] не доверяют самоподписанным сертификатам

---

[14] Можно, например, найти примеры в путеводителях Synergis за 2018 – https://itsynergis.ru/assets/docs/meta_analysis_menaskop_synergis_2018.pdf и 2019 – https://itsynergis.ru/assets/docs/blockchain_cryptocurrency_guidebook_2019.pdf годы.

[15] См. список литературы с манифестами шифропанков и криптоанархистов (В. П.).

[16] Одно из решений – https://unstoppabledomains.com. Аналоги есть у Aeternity, Ethreum, Zilliqa, Namecoin, Emercoin и других.

[17] Речь именно о НЕ-W3-браузерах (В. П.).

и помечают такие сайты как ненадёжные. Почему бы не разработать решение на DLT, где пользователи могут[18] сами заявлять о доверии определённым сертификатам с привязкой к доменному имени?

– Платёжные провайдеры, ограничивающие переводы средств, требуют подтверждения личности, но подвержены взломам и похищению средств.

– Облачные или хостинг-провайдеры – по жалобе заблокируют счёт, сервер, не дадут сохранить данные, могут повысить цену, будут насильно заставлять платить VAT (по мнению отдельных участников рынка, Интернет должен оставаться межгосударственным и межтерриториальным пространством).

– Социальные сети передают (продают!) персональные данные третьим лицам, используют публикуемые материалы и связи для таргетированной рекламы.

– Можно продолжать почти бесконечно…

Безусловно, большинство провайдеров услуг добавляют удобства, взамен – пользователь делегирует право распоряжаться (своими) данными. Добровольно ограничивает себя. Цель многих энтузиастов – донести мысль о том, что в современном мире должна быть и будет альтернатива. Сердцем её является цифровая экономика: децентрализованная, с открытым кодом и доступная для аудита; цифровые сущности

[18] Именно в эту сторону движется https://cyb.ai.

внутри – криптографически защищены.

В 2019 году стала набирать популярность тема совместимости разных блокчейн-систем (interoperability). С появлением HTLC (Hash Time Locked Contract) начали развиваться разные концепции: ILP (Interledger Protocol) или IBC (Inter-Blockchain Communication). Благодаря им в будущем не будет привязки к конкретному[19] блокчейн-решению.

Поэтому термин Web 3.0 сшит с криптографией, контролем за передаваемыми данными, отказом от посредников, взаимодействием в замкнутых системах с собственной экономикой[20]*. Именно в блокчейн-разработках общество видит признаки новой главы Интернета*[21] *– инновации, которая вернёт контроль за данными в руки пользователей.*

Но всё опять не так просто. Общество состоит не только из сознательных людей. Неужели верите в осознанный выбор большинства?[22] Красная таблетка только для избранных, остальные будут рады принять синюю. Сознательный отказ от посредников приводит к самостоятельному контролю: за своими данными, за своими паролями, за своими

---

[19] Хотя есть сторонники другой гипотезы, условно называемой «останется только один», что, на мой взгляд (В. П.), противоречит самой логике децентрализации.

[20] Под замкнутыми здесь имеются в виду полные и независимые экономические модели.

[21] Ещё точнее – эры Постинтернета, поскольку Сеть уже не будет единой (прим. В. П.).

[22] Я – да (В. П.).

средствами, за своими финансами. Готовы ли люди отвечать за свои решения? Сомневаюсь. **А вы?**

Да, осознанным людям новая концепция Интернета даст выбор. «Бесплатно» пользоваться социальной сетью, принадлежащей корпорации, или держать данные на одном из хабов (например, gaia от blockstack), расплачиваясь внутренней криптовалютой за хранение и обработку, а может, и получая токены за просмотр нативных рекламных объявлений (как в Brave). Бесплатно скачивать торрент-файлы, оплачивать повышение скорости или получать токены за раздачу файлов[23] – возможно всё!

***

Большинство не сможет этим пользоваться. Без адаптации в привычные для всех приложения результат определён. Нужен так называемый mass adoption.

Общественная приспосабливаемость возможна в случае принятия правовых норм[24], регуляторных решений и трактовок по разным криптовалютам. Тогда стоит рассчитывать на постепенное внедрение технологий в стандарты, которые имплементируют в браузеры общего назначения (Chrome, Firefox, Opera). Несмотря на то что World Wide Web Consortium (W3C) работает в направлении разработ-

[23] Это стало особенно актуально после IEO BTT (прим. В. П.).

[24] О противоположной позиции читайте в одной следующих глав (прим. В. П.).

ки стандартов по интеграции криптографических инструментов в браузеры, обществу нужно пройти длинный путь по фильтрации концепций и Web3.0-интерпретаций[25].

Компании и разработчики следуют вперёд, используя все доступные средства: как специализированные сайты, применяющие js-библиотеки или браузерные расширения (Metamask и другие web-кошельки) для взаимодействия с блокчейн-системами, так и отдельные приложения (Scatter). В некоторых случаях разрабатываются даже отдельные браузеры (Brave, Puma, CYB). Но всё это может столкнуться с простой цензурой на смартфонах со стороны корпораций, владеющих маркетплейсами (AppStore для iOS, PlayMarket для Android). Например, приложения социальной сети Gab постоянно находятся под блокировками и подвергаются критике в СМИ (естественно, с политическим контекстом, так как речь идёт о свободе слова). Многие приложения, использующие криптографию, не проходят модерацию от Apple и Google. О какой общественной адаптации тогда может идти речь?[26]

Альтернативой приложениям, устанавливаемым через централизованные маркетплейсы, могут являться сами вебсайты, если будут адаптированы и переделаны в прогрессивные веб-приложения (PWA). Подавляющее большинство

[25] Меж тем уже существует и развивается CYB, Beaker и другие проекты, как и дополнения к существующим (прим. В. П.).

[26] Об альтернативной – о чём и шла речь выше (прим. В. П.).

уже поддерживают адаптивную вёрстку. Следующим этапом будет поддержка PWA и взаимодействие с блокчейн-системами напрямую (посредством подключаемых библиотек).

Web 3.0 – вызов всем. Какие технологии будут востребованы? Что выберут пользователи? Могут ли приложения к ДРС быть простыми и доступными? Как ответит финансовый сектор и регуляторы на зарождающуюся цифровую экономику в замкнутых системах?

Вопросы и ответы содержатся в нас. Общество сделает выбор. Каждый.

В поисках новой концепции

В данном разделе представлен список интересных сервисов, связанных с развитием Интернета. Не все заявляют о себе как о Web 3.0, а те, кто заявляют, не всегда предоставляют что-то концептуальное и интересное.

DNS на блокчейне

Хорошо было бы отказаться от посредника-монополиста в виде ICANN. И это возможно именно с применением DPC. Право владения, возможность передачи, заложенная в смарт-контрактах, распределённые DNS-записи[27] – созданы, чтобы одними из первых получить развитие.

ICANN за 20 лет сильно пустили корни в Интернете и уже стали стандартом. Многие просто привыкли, что за домен нужно платить мзду каждый год. Поэтому альтернативы, которые создаются, часто копируют систему, созданную ICANN. Есть как отдельные смарт-контракты, например, eosdns. x на EOS или https://unstoppabledomains.com/ на Zilliqa (а теперь и на Ethereum), так и более универсальные решения (ENS, документация). Сложность заключается в фактическом использовании. Современная Сеть уже полна

[27] Одно из первых решений в этой области – https://ru.wikipedia.org/wiki/Namecoin (В. П.).

правил и механизмов. Безопасность пользователей в браузерах довела до абсурда связь между доменами и SSL-сертификатами (подробности – ниже).

Сейчас норма – использовать https-протокол, но он настолько строго вмонтирован[28] в браузеры, что без разрушения старых правил – новые не построить. Кто-то пытается обойти их в виде расширений (eosdns в Chrome Webstore, исходники), с перезаписью PAC-скрипта для управления прокси. Кто-то вносит правки в сами «просмотрщики» или разрабатывают свой аналог на electron (например, демо от unstoppable). И нельзя точно предсказать, какой подход победит. В EOS, например, есть имена аккаунтов, которые выступают в виде доменных имён[29], и короткие просто так не зарегистрируешь (есть специальный аукцион на конкурентной основе, остатки продают разные сервисы, например, eosnameservice.io).

Вот и получается, что браузеры мешают пользователю, если он идёт на сайт, защищённый персональным сертификатом. Центры же выдают разрешения только за деньги и стягивают на себя такой объём ценности, что просто представить сложно. Появление инициативы Let's Encrypt (в России *заблокировано*[30] Роскомнадзором: всё ради защиты детей!) сильно изменило существующий рынок, но в глобаль-

---

[28] Подробней о стандартах – см. приложение №1.

[29] И не только в EOS (прим. В. П.).

[30] См. подробности https://habr.com/ru/news/t/446398/.

ном плане сложно модифицировать парадигму. Массовому внедрению мешают и действующие нормативы. Только разработка новых сервисов с более гибкими правилами позволит что-то изменить. Для этого нужно:

– пользователям посещать сайты с самоподписанными сертификатами[31];

– доменам хранить в DNS-записях информацию о сертификате, чтобы выявлять вмешательство в виде man in the middle (для специалистов: да, конечно, для бизнеса в реальном мире хочется иметь «знак качества» от третьей стороны, в современном мире этим занимаются сертификационные центры, но для обычного использования уже доступен Let's Encrypt, который выступает поверенным, что сертификат сформирован на сервере и прошёл проверку размещением файлов определённого содержания. Стоит отметить, что домен и сервер, который его обслуживает, – две разные сущности, обслуживаемые обычно одним владельцем, поэтому считаю TXT-запись в домене слепком сертификата, достаточным для проверки и защиты от man in the middle. В таком ракурсе поверенные нужны для утверждения, что сертификат соответствует определённому юридическому лицу в реальном мире);

– user'ам голосовать своим стеком/активностью в публичных блокчейн-системах, проявляя таким образом доверие такому сертификату;

[31] И/или изменить саму систему создания таких сертификатов (прим. В. П.).

– устанавливать расширения для работы с scheme (например, для ввода нового пространства имён eos://) и прозрачно делать https-запросы по определённым в блокчейне ip-адресам.

Закрадываются сомнения: сделают ли это лидеры рынка браузеров? Или они работают на интересы групп ICANN и разных CA (Certification Authority, список от Mozilla Foundation)?

Возможно, это будут совершенно новые браузеры или модификация существующих, но под иным брендом. Только время покажет, какой из экспериментов выживет и даст пользователям необходимую гибкость.

P. S. Для вопросов по децентрализации SSL-сертификатов рекомендую изучить Remme и DNSChain (сервер с поддержкой Namecoin). Сводка по ценам на домены в блокчейн-системах – peername.com.

Взаимодействие сайтов с блокчейн-системами

Если со сложными консольными приложениями разобраться могут не все, то массового потребителя можно привлечь через простые и понятные разработки. К таким стоит отнести веб-приложения (или их обёртку в виде полноценных приложений для разных операционных систем) и брау-

зерные расширения.

Веб-приложения, которые держат данные в хранилище браузера, работают по определённым принципам: зашифровывают приватные ключи для безопасности, позволяют завести несколько аккаунтов или адресов для быстрого переключения между ними, имеют предустановленные возможности для конкретной системы (зачастую это получение информации об активном аккаунте или адресе, инициация подписи данных, запрос на отправку токенов) и настроены на взаимодействие с конкретными публичными нодами.

Интеграция с веб-сайтами – непростая задача, но вполне решаемая с помощью расширений, например, того же Metamask для Ethereum или Waves Keeper для Waves. Часто аддоны выполняют роль кошелька и трансформируются в десктопные приложения через Electron, так как сталкиваются с цензурой маркетплейсов (так, например, и случилось с Scatter для EOS).

Механизм работы интеграции обычно выглядит так: подключение js-скриптов для передачи данных расширению или приложению, сайт инициирует запросы, приложение запрашивает подтверждение у пользователя и транслирует его решение обратно. Часто этот процесс и называют Web-3, так как происходит взаимодействие стороннего сайта с блокчейн-системой через приложение, которым управляет пользователь.

Подобные инструменты решают проблемы авторизации,

отказа от посредников, где двухфакторная аутентификация заменяется паролем для подтверждения операций или интеграцией с Hardware Wallet (Ledger или Trezor).

Децентрализация провайдеров

Любые посредники могут быть заменены p2p-системой с внутренней экономикой. Интернет-провайдеры находятся в зоне риска из-за развития IoT (Internet of Things), 5G, mesh-сетей. Несмотря на то что теми же mesh-сетями интересовались энтузиасты давным-давно, популяризация блокчейн, развитие смежных технологий, таких как 5G, и потенциальное покрытие спутниковым Интернетом всё больших территорий позволили появиться проектам, которые заявляют о себе как о децентрализованных mesh-сетях. Заявки серьёзные – для многих это выглядит как далёкая фантазия: расшарить Wi-Fi, связаться с другими узлами, получать вознаграждение за связность сети и предоставление услуг передачи данных, пользоваться сервисами других провайдеров, оплачивая их аналогичными токенами. В этой фантазии замечательно всё, но возможна ли она – покажет время. Многие проекты, которые собирали средства через ICO, ещё демонстрируют признаки жизни (SmartMesh, RightMesh, AMMBR). Возможно, на их фоне (и на фоне открытых разработок) будут взращены те, что докажут свою жизнеспособность и необходимость всеми миру.

Децентрализация хранения данных

В эпоху Web 2.0 развитие получили облачные провайдеры. Пионеры в этом – Amazon Web Services (AWS): довольно крепко закрепились на рынке услуг, в том числе в cloud storage. И если Dropbox, iCloud, Google Drive, Яндекс. Диск в первую очередь были нацелены на retail-услуги (для конечных пользователей), то корпоративный сегмент заняли SaaS-решения. Так, S3 от AWS и часть других CDN полностью захватили рынок. Конкурировать с ними по распределённому хранилищу, резервному копированию и доступности (uptime) стало сложно. Корпоративный подход свёл ситуацию почти к монополии между крупными корпорациями. Новым провайдерам сложно запускать какие-либо услуги, так как предоставить какие-то конкурентные преимущества попросту невозможно. И тут на сцену вновь выходят ДРС.

IPFS стал первым успешным примером работы распределённой файловой системы (про торрент чуть позже). Несмотря на отсутствие экономики в IPFS, протокол популярен: на нём создают сайты, которые обращаются к файлам, скриптам и другим элементам через IPFS-шлюзы (публичные провайдеры, готовые кэшировать и предоставлять доступ к файлам из IPFS посредством HTTP- и HTTPS-протоколов). В связке с возможностью обращения к публичным нодам различных блокчейн-систем через JSON RPC такие

сайты стали своего рода децентрализованными.

Основная проблема подхода – отсутствие экономического стимула содержать IPFS-ноды и публичные шлюзы (всё пока на плечах или, точнее сказать, «кошельках» энтузиастов и идеологов). Поэтому есть проекты, которые ставят своей целью решить данную проблему, например, FileCoin и BTFS (который будет использовать токен BTT на сайдчейне TRON). Проблем, связанных с хранением и доступностью файлов, как технологических, так и экономических, – много. Посмотрим, какой подход найдёт больше сторонников и займёт часть ниши, но нужно понимать: старая парадигма с облачными решениями никуда не денется. Часть рынка в виде потребителей может перейти на новые, что изменит экономику всей экосистемы. Циркуляция данных, их ценности и способ оплаты услуг – всё будет постепенно уходить из централизованных финансовых систем, лишая посредников как комиссий за переводы, так и возможности взимать налоги за предоставление услуг в привычном для текущего мира понимании (например, VAT в России составляет 20%[32]).

[32] НДС – не единственная проблема в РФ и во многих других государствах: есть нечестная таможенная политика, из-за которой покупки в зарубежных онлайн-магазинах год от года не становятся дешевле; существует ряд законов, постепенно делающих дороже конечную стоимость товаров и услуг (закон Яровой в первую очередь) и т. д. (прим. В. П.). И хочется верить, что ДРС не станут панацеей, но помогут вернуть конкуренцию.

Децентрализация идентификации и репутации

В настоящее время мало проектов занимаются репутационными моделями. Зачастую они носят локальный характер (внутри определённого сообщества или замкнутой модели оценки). Методология расчётов может быть сложна или наоборот – вызывает вопросы своей простотой. Часто в подобных системах обсуждается центр сертификации, своего рода паспортный контроль для учёта аккаунтов после прохождения KYC.

Транслировать в новую парадигму распределённых реестров старые принципы – *пустое и бестолковое занятие*. Как только возникает вопрос учёта голосов из реального мира, например, при участии в выборах, сразу технически подкованные люди хватаются за голову.

Старый подход в виде «1 персона имеет 1 голос» – может и кажется социально справедливым, но совершенно не подходит для учёта заинтересованности сторон. Компромисс в виде социального уравнивания подходит государству, но в цифровом пространстве вызывает вопросы.

Поясню: экономика в распределённом реестре – центр экосистемы. Почему аккаунт с 0,01 токена даже в теории должен иметь аналогичный по весу голос по сравнению с держателем 100 токенов? Это банально несправедливо, так

как заинтересованность в благополучии и работоспособности системы у второго выше в 10 000 раз!

А системы дропов в реальном мире, когда люди продают свою личность для получения банковских счетов, адреса для любых посылок или телефонные номера? Именно в распределённом реестре с экономическим ассетом человечество начинает просыпаться и осознавать необходимость долевого голосования[33]. Почему система в реальном мире зачтёт голос продажного пьяницы, а суд проигнорирует нападки этого же пьяницы на репутацию другого человека (не дал на выпивку)? Двойные стандарты?

В цифровых системах аккаунтом может владеть не человек, а робот[34] (или умное устройство, например, музыкальная колонка). Более того, аккаунт может принимать решения в сети, защищая свои интересы. *И внутренние механики не должны ограничивать роботов в цифровых правах*. Как только появляется идея ограничить аккаунты участием в голосовании в виде требования прохождения верификации и выдачи сертификата (или паспорта) – можно сразу ставить крест на подобной системе: уже на этапе проектирования имеем уязвимое место – центр верификации или выдачи сертификатов.

---

[33] Исторически возвращаемся в эпоху XVII – XIX вв., когда имущественный ценз был, но совершенно по иным основаниям (прим. В. П.).

[34] Напомню, поэтому в глоссарии указан SaO – субъект и объект, как единая сущность, выступающая в ДРС (см. подробней ниже – В. П.).

Покупка голосов, коррупция, злоупотребления на местах – пережитки старых систем, которые старались социально уравнивать персон. В цифровом пространстве с собственной экономикой доверять можно тем, которые основаны на справедливом долевом участии, где серьёзность намерений можно доказать заморозкой активов на длительный срок.

Системы идентификации носят больше рекомендательный характер, так как не могут гарантировать честность посредника (проверяющего и удостоверяющего центра). Например, существует проект KeyBase, который используют сами пользователи, предъявляя доказательства (криптографического, естественно, характера) связанности своего аккаунта со своими профилями в социальных сетях.

Протоколы взаимодействия

Бурный рост проектов с использованием распределённого реестра привёл к новой проблематике – как связать их воедино? Как добиться их взаимодействия, желательно бесшовного? Постепенно энтузиасты нашли решение в виде Hashed Time-Locked Contract (HTLC, также известные как атомарные свопы) и его разновидностей. С рождением возможного решения выявились и новые проблемы:

– Как связать два блокчейна?

– Что будет делать проверяющая сторона – обращаться

в другой блокчейн?

– На чём будет основано доверие другой ноде и её состоянию? Верю – не верю?[35]

Логика подсказывает, что нужен какой-то доверительный узел или канал связи между разными блокчейнами. И тут либо работать напрямую с узлами сети (доверие или проверка через нескольких оракулов), либо через посредников (шлюзы, которые будут играть роль доверенных хранителей токенов, выполняя роль custodian-сервисов). В итоге имеем два разных подхода: ILP (Interledger Protocol) и IBC (Inter-Blockchain Communication). Вполне вероятно, что оба докажут свою жизнеспособность и будут использоваться[36]. Взаимосвязь разных распределённых реестров – часть W3-концепции. Web 2.0 научился жить с аутентификацией через другие сайты (OAuth), Web 3.0 не останется в стороне, только уже в современном Интернете с сотнями блокчейн-систем.

Codius – слон, не видимый в комнате?

Перед тем как состоялся Ethereum, в лаборатории Ripple родился Codius. Codius превратился в самостоятельный проект и после появления блокчейн-платформ со смарт-кон-

[35] Каждый из этих вопросов раскрывается по-своему в главах ниже (В. П.).

[36] Скорее всего – их будет на каком-то этапе и многим больше (прим. В. П.).

трактами был временно заморожен. Пока мир не распробует набравшую популярность виртуальную машину[37] «Эфириума», нет смысла концентрироваться на «Кодиусе». Но трудно его игнорировать, так как успешная имплементация в современные финансы может составить значительную конкуренцию любым ДРС.

Идея в том, что построение смарт-контрактов может быть выполнено вне блокчейн-окружения. Добавить скриптам распределённость, взаимодействие с платёжными инструментами (такими, как Interledger Protocol) – и для взаимодействия участников контракта это будет проще, чем работать в рамках блокчейн-платформы. Почему проще? Потому что стоить будет гораздо дешевле, поиск исполнителей расширится до веб-разработчиков, позволяя опираться на данные вне блокчейн-окружения (отсутствие аналога оракулов – большая проблема в текущем поколении p2p-систем).

Codius – своего рода открытая платформа для продажи в аренду серверных ресурсов и мощностей. Запущенная и настроенная, она автоматически принимает оплату от инициатора, разворачивает у себя Docker-контейнер с необходимым окружением и берёт плату за использование ресурсов. Можно назвать Codius хостинг-провайдером для приложений в контейнерах. И это отличное описание.

Проект явно опередил время и теперь ждёт своего ча-

[37] Или любой её аналог (В. П.).

са. Уже сейчас блокчейн-сервисы, предоставляющие исполнение смарт-контрактов, задумываются о пиковой нагрузке. Учитывая общий распределённый реестр и характер формирования блоков, можно сказать, что вся активность на подобной блокчейн-платформе ограничена одним топовым сервером. Создание и разделение цепи на пара/сайд/подцепи (шардирование)[38] поможет. Но стоит понимать, что ограничения в рамках одной платформы никуда не денутся (вычислительные ресурсы общие). И переплачивают за это конечные пользователи (комиссиями за транзакции) или создатели приложений, арендуя мощности за счёт заморозки токенов, которые подвержены инфляции.

Именно проблема в виде масштабирования и подтолкнёт сообщество к изучению альтернатив в виде Codius. Smartcontracts на любом языке программирования в Docker-контейнере возможны: одним из таких примеров является проект Hot Pocket (GitHub) – прототип универсального распределённого реестра со смарт-контрактами.

Сейчас же сервис ждёт: нужно всестороннее развитие контейнеров (Kubernetes и Kata Containers), Web Payments, внедрение и расширение охвата Interledger Protocol и критическая нагрузка на блокчейн-платформы (EOS, например, пострадал от таковой, создаваемой смарт-контрактами EIDOS в 2019 году, а Ethereum – в 2017). Поэтому слону, Codius торопиться не надо – он уже давно в комнате и его

[38] Читайте подробней в главах ниже.

определённо заметят.

W3C: Web Payments и Web Authentication

Нынешний Интернет настолько связан с разными протоколами и услугами посредников, что вопрос выживания того или иного подхода лежит уже не в плоскости технологий, но в стандартизации и имплементации в существующие решения. Именно вторым и занят Консорциум Всемирной паутины, он же World Wide Web Consortium, он же W3C. Рекомендации именно от W3C находят применение в современных браузерах. Google, Mozilla Foundation, Opera – малая часть участников W3C, полный же список можно найти на официальном сайте (их около 460).

Конфликты внутри таких объёмных объединений неизбежны, поэтому в 2004 году представители индустрии основали WHATWG (GitHub), которая перетягивала стандартизацию HTML5 на себя, и только в 2019 году стороны подписали меморандум, который представлял компромисс.

Когда говорим о Web 3.0 и размышляем о судьбе распределённого реестра, стоит задуматься: какие именно технологии дойдут до конечного потребителя (массового пользователя)? И через какие инструменты?

Логично предположить, что браузер – краеугольный камень во всём этом процессе. С развитием WebAssembly и его поддержки технологическими гигантами – вполне

возможно, что нативные приложения постепенно перейдут в браузерное окружение. Поэтому стоит присмотреться, кто из существующих пионеров блокчейн-технологий взаимодействует с W3C. Изучив список членов, можем найти представителей:

– Ethereum Foundation (ETH);
– Brave (BAT);
– Ripple (XRP, ILP);
– Coil (ILP);
– ConsenSys (ETH);
– Facebook (Libra).

Именно они работают над стандартами для того, чтобы создать условия простого взаимодействия с пользователями. И основными направлениями для стандартизации технологий, связанных с блокчейном, являются Web Payments (сайт рабочей группы) и Web Authentication (сайт рабочей группы).

Стандарт Web Payments даёт спецификации (Payment Request API, Payment Method Identifiers, Payment Method: Basic Card, Payment Handler API, Payment Method Manifest) для платежей в Интернете через браузеры (вводное руководство от Google). Уже сейчас Chrome и Firefox позволяют запоминать введённые данные с пластиковых карт, что значительно ускоряет покупки через тех или иных агентов. Предполагаемый стандарт позволит проводить транзакции про-

ще и быстрее как для получателя средств, так и для пользователя. Учитывая наличие в рабочей группе представителей Facebook, можно говорить об интеграции не только в браузеры, но и в целевые приложения, связанные с большим количеством пользователей[39] (социальные сети). А наличие ISO 20022 Registration Authority подчёркивает важность данного стандарта (именно ISO 20022 объединяет разработки из современного мира финансов).

Блокчейн-компании и программисты сами порождают свои механизмы оплаты, пусть и без сохранения единого стандарта. Так, например, в bithomp.com есть возможность войти, используя холодные кошельки от Ledger, Secalot и Ellipal. А большинство сервисов для EOS требуют наличия приложения Scatter. Увидим ли в будущем адаптацию стандарта Web Payments для поддержки криптовалют – не знает никто, но упрощение процесса, устранение посредников и высоких комиссий в уже привычных феноменах может значительно повлиять на привычный Интернет.

Стандарт Web Authentication ставит целью дать браузерам (и их пользователям) единую спецификацию для взаимодействия сайтов с комплексом инструментов (и, надеюсь, единым интерфейсом), связанных с внешними аппаратными носителями (через USB, Bluetooth или NFC)[40]. И если с совре-

[39] Впрочем, не стоит забывать и о проблемах Libra (В. П.).

[40] Подробнее почитать о нём можно в статьях threatpost.ru, hype.ru, habr.ru и ещё habr.ru.

менными смартфонами не возникает вопросов (туда всё чаще встраивают чипы и технологии для сбора биометрии), то с персональными компьютерами всё непросто. Опять опираемся на агентов в виде сертификационных центров, поэтому стандарт уже ограничивает блокчейн-имплементации, которые могли бы как раз заменить этот слой. Не удивляйтесь, если в будущем стартапы наподобие BiChip (twitter), которые вживляют в руку RFID/NFC-чип, захватят мир, начиная с Африки. Зачем людям кошелёк, когда можно приложить руку (в настоящем – смартфон) к считывающему устройству?

Подводя итоги, можно выразить надежду, что блокчейн-компании и энтузиасты смогут отстоять хотя бы малую часть аутентичности. Иначе разного рода посредники навсегда сохранят своё положение в мире.

DeFi: децентрализованные финансы

Криптовалюты позволили людям отказаться от оравы централизованных посредников при передаче ценности, оставив операторов учёта (майнер, блок-продюсер, делегат). Это послужило мощнейшим толчком для развития как технологий, так и финансовых взаимоотношений. Переводы токенов набирали обороты и при росте общей капитализации рынка выстрелили в современный мир финансов.

DeFi – открытые инструменты или протоколы в распреде-

лённых системах, так или иначе решающие какие-то финансовые задачи. Часто у конкретного решения есть свои члены правительства, которые принимают решения по управлению параметрами системы.

DeFi на момент написания данных строк больше воспринимается как смарт-контракты и возможности в той или иной блокчейн-системе, которые предоставляют финансовую услугу. Даже есть целые ресурсы, которые делают списки из подобных проектов, ведут рейтинги. Аналитики выделяют несколько категорий DeFi:

– Decentralized Exchanges (так называемые распределённые обменники, они же DEX) и открытые протоколы обмена (0x, UniSwap, Kyber Network, Bancor Network, Ren, IDEX, BitShares);

– Lending and Borrowing (кредитование и заимствование: MakerDAO, Compound, Dharma);

– Derivatives, Margin Trading & Prediction Markets (деривативы, маржинальная торговля и рынок предсказаний: Augur, CDx, dYdX, bZx, Daxia).

Особенность DeFi в единой распределённой системе – возможность взаимодействия протоколов друг с другом и производными токенами. Именно поэтому наибольшую популярность DeFi получили на Ethereum.

Но на фоне уже разработанных продуктов и инструментов происходит кое-что другое: идёт подготовка существую-

щего финансового мира к вступлению в игру на рынке систем распределённого реестра. Множество крупных компаний, сотни и тысячи разработчиков трудятся над переносом потребностей современного человечества. Достаточно открыть список клиентов и партнёров того же R3 (Википедия) или Hyperledger. Разработки ведутся во всех направлениях:

– Страхование? Есть.

– Идентификация? Есть.

– Торговля металлами? Есть.

– Клиринговая палата? Есть!

– Патенты, здравоохранение, медицинское страхование? Всё это есть.

– Кредитование? Тоже есть.

Важно! Всё это уже не просто прототипы – это реальные сервисы, которые ждут одного: одобрения[41] регуляторов. Как только это произойдёт – станем свидетелями массового перехода существующего мира на новую парадигму. И вместе с провайдерами услуг на рынок хлынут их клиенты с деньгами в виде ценности, объём которых превышает текущую капитализацию криптовалют во множество раз. Нас ждёт много интересного после конца 2019 – начала 2020 года, но уже сейчас можно встать на ступеньку выше и окунуться во вселенную распределённых финансов. Нужно лишь начать ин-

[41] На мой взгляд – только новых пользователей (В. П.).

тересоваться и изучать. Благо, информации так много, что надолго хватит.

Послесловие к главе первой

Усиление централизации до абсурда, монополия технологических гигантов, смена парадигмы бизнеса и концентрация внимания на рынке услуг, где люди – товар в том или ином виде. Эволюция технологий приводит нас к очередной развилке. *Идти подобным путём или выбрать децентрализацию?*

Возобновляемые источники энергии, саморазвитие, самоуправление, самодисциплинирование, самоосознание? Префикс «само…» не всегда значит в одиночку. *Он значит осознанный выбор и действие*. Единомышленники найдутся и сплотятся там, где необходимо. Децентрализация – не про «переложить ответственность», а именно про «взять её на себя». Многие забывают об истинном значении слов. Интернет – не исключение.

Кто-то воспринимает Web 3.0 по методичке тех, кто его подготовил. Безусловно, есть много взглядов на то, что такое Web 3.0. В блокчейн-технологиях чаще встречаем упоминание этого термина в связке с проектами Ethereum, Cosmos, Waves, BlockStack, Polkadot, IPFS. Но по-настоящему независимыми и свободными можем стать, только если поднимем свои сервера и будем хранить информацию тоже сами. Невозможно отказаться от FB и отправлять фотографии родственникам без хранения и передачи файлов. Кто их бу-

дет хранить, кто будет передавать, какие у них будут экономические стимулы? Кто, если не вы?

Web 3.0 и блокчейн – не волшебная таблетка[42] и не решение всех проблем. Хранение данных стоит денег (или другой ценности). Передача данных по каналу (трафик) стоит денег. Содержать инфраструктуру серверов тоже стоит денег (даже такие распределённые сервисы, как Mastadon, требуют электричества для работы сервера, самого сервера и оплаты канала связи).

Общество прошло тот этап, когда бесплатный сервис, широко улыбаясь, не использовал ваши данные: бесплатные сервисы успешно выжидали, наращивая пользовательскую базу, и искали бизнес-модель. Теперь они успешно продают: **вас**.

Альтернатива – замкнутые экономические модели, где прозрачны правила игры для держателей инфраструктуры (администраторы, майнеры, валидаторы, блок-продюсеры – получают часть от эмиссии), сервисов (веб-клиент, веб-сервис, блок-эксплорер, интерфейс к данным – показывают рекламу) и для самих участников сети (пользователи сервиса, сайта, услуги – вознаграждение за действие, покупка токенов для усиления влияния, оплаты услуг или комиссий системы). Отказ от излишних посредников или взаимовыгодное открытое соглашение.

Вот что такое *Web 3.0, помимо технологий – концепция*

[42] Но и не плацебо (В. П.).

выбора и свободы.

Глава II. Карта местности – архитектура Web 3.0, или О чём не стоит забывать

Автор данной части – криптоэнтузиаст, ecosystem development lead в cyber~Congress, основатель консалтингового агентства Blocksult Сергей Симановский. Контакты: @serejandmyself.

Великая паутина

Давайте начнём неправильно. Давайте начнём с того, что эта история не расскажет. Моя история не расскажет, как разбогатеть. Она не расскажет, как быть успешным. Но она расскажет о том, как с помощью растущей (и давно существующей) технологии стать *свободным*. Жить в довольно простом мире. Чувствовать себя нужным. Слышится так, будто это не те ценности, которые пытаемся изменить с помощью технологий. Но тогда что?..

Web 3.0, или Великая паутина, – коммуникационная структура, если можно так сказать. Взаимосвязь старых и новых протоколов, технологий и алгоритмов, которые переносят (нас) в прошлое. Почему именно в прошлое? Потому что так же, как и Bitcoin, W3 – реверсивный стек. Он возвращает к истокам с помощью технологий. То, что было так долго недоступно для многих, теперь становится общепринятым[43].

Один из моих любимых вопросов: где размещается W3? Является ли это приложением? Является ли это сетевым протоколом? Да, немного всего этого сразу.

Но начнём с начала: Bitcoin. Bitcoin помог людям понять текущую финансовую систему: мы должны отвечать за свои финансы и не доверять никому другому.

Является ли Bitcoin частью W3? Думаю, да. Blockchain

[43] Со временем – общеупотребимым (прим. В. П.).

в целом является частью Web 3.0. Что-то, что позволяет общаться app-2-app. Peer-2-Peer. Сеть-2-Сеть. Но разве блокчейн не является прикладным уровнем? Да, это наверняка так, но и наверняка НЕ так. Blockchain одновременно является приложением, но может быть и протоколом взаимодействия: может быть шифровальным уровнем в целом. Но дело не в этом.

Закончим введение и перейдём сразу к пониманию того, кто является крупнейшими игроками за столом в данный момент. И попытаемся понять, как W3 работает на более высоком уровне.

Как говорил выше, W3 функционирует, помогая идейному вдохновителю действовать напрямую, без посредника. Он отменяет цепочки больше трёх: HTTP, DNS и URL, – позволяя общаться напрямую.

Почему коммуникация важна?

Коммуникация – абсолютный и самый важный протокол. Это то, как функционируем, думаем, рождаемся, умираем, обмениваемся деньгами, сигналами и т. д. Коммуникация – всё. Мы – социальные существа. Как и другие существа на нашей планете и, возможно, за её пределами.

Большие пушки

Несколько игроков W3 могут помочь понять, как этот феномен работает сейчас и как он (вероятно) будет работать в будущем. Давайте рассмотрим их и попробуем построить технологический стек, который поможет осознать, как можем создавать глобальные сети, от аппаратного обеспечения до персонального блога на вашей собственной (!) операционной системе.

Постараюсь разнести проекты по блокам, по категориям и опишу, что они сделают в кратчайшие сроки по отношению к W3 и как это поможет построить новый коммуникационный протокол.

Во-первых, Bitcoin – новая глобальная валютная система. Деньги, которые не требуют третьей стороны. Деньги, которые всегда отправляются: независимо от цели. Деньги без границ, которые функционируют 24 часа в сутки 7 дней в неделю: без удостоверения личности, банка или любой другой сущности («any other bingo bullshit»). Bitcoin закладывает основу для нового коммуникационного стека, на котором можем строить (что угодно). Мы общаемся через деньги. Говорим о деньгах. Это наш язык. Наш базовый протокол.

Polkadot и Cosmos – возможно, должны быть последними в моём списке, но это не так. Что они позволяют – так это создать по-настоящему интероперабельную систему свя-

зи: ту, в которой можем передавать ценность между сетями безо всякого беспокойства. Там, где владеете своей сетью, если хотите. И можете поделиться сетью с другими. Но главное – можете общаться со всеми безопасным и очень эффективным способом.

Polkadot и Cosmos важны, потому что они обеспечивают столь необходимое соединение между автономными блокчейнами, приложениями и протоколами, развивая необходимый сервис. Если Bitcoin – деньги, то этих двоих можно рассматривать как маршрутизаторы, которые помогают передавать информацию.

Отдельная часть головоломки, которую необходимо упомянуть, – IBC от Cosmos. IBC[44] – протокол, который склеит все «чейны» Tendermint вместе: позволит осуществить одну простую, но мощную вещь – передачу данных между цепочками (следует отметить, что на момент написания этой главы IBC уже протестирован и готов к окончательному публичному тестированию через 1—2 месяца).

Передача данных при этом может означать и передачу токенов. Токены – технические данные внутри конкретного блокчейна. Если распахнёте свой разум и подумаете о бесконечных возможностях, которые может создать подобный подход, – сильно удивитесь! Скажем, если блокчейн имеет какую-либо утилиту (нас не интересуют те, которые не интересуют), то можем сделать обмен: по любой цене / набо-

[44] См. также выше (В. П.).

ру правил и на любую схожую сущность. Пусть мой блокчейн производит рейтинг для контента, а ваш – создаёт репутацию для писателей: теперь же можем установить правила торговли между двумя упомянутыми ДРС. Но так как объём проектов практически бесконечен, сие дарует уникальную возможность и для бесконечных (новых) рынков.

Есть много потрясающих и эффективных, современных, компьютеров, о которых нужно упомянуть, говоря о W3: Ethereum 2.0, Aeternity, Cardano, Holochain и другие. Это автономные двигатели, которые работают в одном направлении: создают экосистемы, в которых могут участвовать программисты, – с открытым исходным кодом, предоставляя нужные инструменты для работы. Они создают столь необходимую инфраструктуру для децентрализованных приложений (Dapps), которые могут напрямую взаимодействовать друг с другом с помощью вычислительных правил и кода. Каждое из оных имеет отличную точку зрения на технологическое восприятие окружения. Но реальность такова, что все они – цепочки общего назначения и делают один и тот же трюк – дают нам (нужные!) инструменты.

IOTA и FOAM – два удивительных проекта с миссиями мирового значения. Оба могут быть размещены в пространстве Интернета вещей. IOTA пытается децентрализованно установить связь между всеми устройствами в мире, а FOAM хочет составить основу инновационной картографии, которая, в свою очередь, даёт свободу в таких направ-

лениях, как логистика, геотегирование и т. д.

Aragon – проект, который призван создать свободную юрисдикцию (вернее, убедиться, что единственная юрисдикция – код) для организаций. Стоит понимать, что нам нужны какие-то системы управления. Локальное управление будет иметь (первичную) тенденцию. На протяжении всей истории местные общины процветали и функционировали лучше (Швейцария, Лихтенштейн, Люксембург, Монако и т. д. остаются одними из самых богатых и счастливых стран в мире на сегодняшний день) иных. «Арагон» помогает сформировать судебные системы, организации и многое другое, а общинам предоставляет возможность самоуправления.

Decentraland. Собственное царство. Не без минусов и препятствий, но тем не менее проект с огромными амбициями. Помечтайте о полностью цифровой и виртуальной реальности. Той, которая защищена от бюрократической и утомительной скуки современного мира. Это виртуальная реальность высшего порядка: место, где люди могут найти убежище от суеты мира. Начните новый бизнес, установите новые правила, создайте города и районы, где только позволит воображение – сквозь горизонт.

IPFS и Filecoin. Возможно, самые важные упоминания в этом списке. IPFS – протокол, который создан для того, чтобы сделать Интернет быстрее, безопаснее и открытее. IPFS позволяет распространять большие объёмы данных и хранить каждую версию файлов. IPFS упрощает на-

стройку сетей для зеркалирования данных. Это означает, что данные практически неизменны, а если возможно – то и вечны. IPFS способствует дальнейшему распространению сетей среди коллег (пользователей). Она обеспечивает постоянную доступность – с интернет-подключением или без: помогает обмениваться файлами и просматривать их, управлять большими кусками данных, создавать приложения и т. д.

С другой стороны, Filecoin – проект, целью которого является внедрение IPFS в массы. Это рынок данных. Неиспользованные ресурсы, лежащие в основе большинства домашних хозяйств[45] в современном мире. С помощью экономических механизмов и посредством IPFS Filecoin может стать первым проектом, которым будет использоваться в ближайшие годы всякий, кто даже никогда и не слышал слово blockchain.

Cyber создаёт совершенно новый протокол для добавления и поиска информации на графе знаний (компиляция фактов о чём-то, что наполняется смыслом). И ранжирует эту информацию. Различные типы пользователей создают связи между IPFS-хэшами и размещают их на графе, тратя так называемые пропускные полосы[46] (количество данных, которое может быть передано за определённый период времени). Затем контент динамически ранжируется с по-

[45] Оставил именно такой перевод как отсылку к началам экономической теории (В. П.).

[46] См. также https://ru.wikipedia.org/wiki/Пропускная_способность (В. П.).

мощью цифровых маркеров и текущих параметров нагрузки сети. Это делает ранжирование динамическим[47] (то есть оно характеризуется постоянным изменением, активностью или прогрессом).

Всё это вычисляется программой или компьютером, который отвечает за проверку достоверности чего-либо. Валидаторы делают это с помощью вычислительных ресурсов. Это позволяет искать данные в сети, ранжировать их, делать запросы и создавать базы данных знаний без посредников и/или «чёрного ящика» (третьих лиц, которые пытаются цензурировать информацию, скрывать или подсовывать определённые результаты, чтобы получить вознаграждение, отслеживать данные и т. д.).

«Кибер» использует DURA (распределённый единый адрес ресурса), который является эквивалентом URL (аббревиатура для унифицированного локатора ресурсов), который видите в браузере при посещении W2-сайта. Вся идея DURA проста: просматривайте контент, не полагаясь на какие-либо реестры (ICANN). Это означает, что не будете рассчитывать на третью сторону при маршрутизации пакетов. Никакой цензуры и т. д. Кроме философского вклада, DURA поможет обеспечить безопасность, глобальность и постоянную связь на нужном уровне.

Гиперссылки формируют Интернет. Они его построили. Мы же основываем наши знания, наши политические, эко-

[47] О важности транзакционной репутации – читайте ниже (прим. В. П.).

номические и образовательные решения на Сети: учимся у Google. Google – наш отец, учитель, источник знаний, социальная жизнь и т. д. Но как можем доверять Интернету, если он был сформирован чем-то, что само по себе не вызывает доверия? Не можем. Киберссылки, с другой стороны, верифицируются и поддерживаются проверенными и проверяемыми механизмами. Это означает, что с их помощью можем создать доверенную модель всей информации во Вселенной!

Страницы (содержимое) добавляются в индекс, когда кто-то отправляет CID или создаёт киберссылку. Это транзакции (они требуют той самой «полосы пропускания», которая служит механизмом защиты от спама). Транзакции проверяются валидаторами (компьютерами, которые обеспечивают баланс для отправки транзакции) и добавляются в граф, к которому затем обращается тот, кто делает запрос в базу. Страницы ни в коем случае не исключаются из индекса. Каждая транзакция важна и должна быть маршрутизирована (передана по назначению, какой бы она ни была).

Cyb – дружелюбное приложение-робот / персональный браузер. С одной стороны, простой браузер. Но это не так. Проблема в том, что на данный момент нет такого слова, которое бы описывало, что такое Cyb. Это браузер в том смысле, что он позволяет искать нечто (какие-то «вещи»). Но это и ваши личные приложения, которые могут понять многое другое: например, Cyb может действовать как кошелёк; как

база данных; содержит ваших киберпространственных роботов. И да, он работает через DURA, а не через обычный DNS/HTTP/URL и с помощью полных узлов маршрутизации информации между собой и пользователями.

Интересно, что такой простой механизм позволяет создать множество мощных инструментов. Например, унифицированная семантика, инструменты SEO, автономные роботы, доступ к собственной базе знаний и многое другое. Наряду с IPFS, Cyber формирует самый важный рынок будущего – обмен информацией. Это золото, нефть и бриллианты завтрашнего дня. Идея заключается в том, что Поиск – глобальный механизм, который понятен всем независимо от языка, расы, возраста и т. д. Это в некоторой степени основной инстинкт (поиск пищи для выживания и т. д.). В цифровом мире с помощью поиска получаем ответы на вопросы, которые всегда задаём. Поиск помогает построить модель вокруг любой интересующей темы. С помощью него можем создать базы, которые могут привести к большому количеству полезных инструментов.

Urbit. Один из самых безумных проектов в дикой природе. «Урбит» – своего рода последний рубеж для W3 и децентрализации в целом. Наряду с такими проектами, как Cyber, IPFS и другие, способен полностью изменить игру.

Urbit – персональный защищённый сервер с вашей (!) операционной системой и идентификатором. Подумайте об этом. Мир контролируется такими компаниями, как

Amazon, которые ввели надзор за самыми большими кусками информации в мире (хостинг серверов CIA и другие государственные серверы). Могут ли все эти проекты стать децентрализованными, если стоящие за ними вычисления принадлежат одним и тем же гигантам? Нет. «Урбит» намерен изменить это. Более того, это совершенно новый технологический веб-стек, меняющий облик компьютерной науки с помощью своего языка Hoon и минималистического подхода к системам.

Неужели всё это звучит слишком, чтобы принять? Да. Необъяснимо, но так и есть. Уже обрабатываем за день больше информации, чем люди 100 лет назад за жизнь! Чтобы идти в ногу с развитием, должны желать учиться. Но как это связано с W3? Что ж, давайте сделаем ещё один шаг назад.

История жизненно важна

Если масштабируем известную историю по годовому календарю (13,2 миллиарда лет, которые можем наблюдать), то вся она помещается в последние 7 секунд. Это включает в себя целые цивилизации, войны и т. д. Современная история… мгновение ока.

Точка зрения проста. Если хотим перемен, то должны учиться, должны тратить время, чтобы понять, что долго говорили об идеях прямого общения, частных деньгах, свободном мышлении и т. д., которые были рядом с нами столько, сколько знаем (себя). Сегодня наконец-то появилась удивительная возможность использовать технологии для реализации этих идей.

Не могу оставить без внимания аргументы, которые слышу от многих (увы, из-за отсутствия необходимых знаний). Перечень их таков.

«Хорошо, понимаю, что W3 – сочетание всех сервисов, которые когда-либо хотели, – частных денег, свободы слова, удивительных технологий и всего остального… Но… что будем делать, когда вырежут Интернет, а?»

Обычно на этом этапе спорящий человек выглядит таким счастливым, что одержал победу над всеми идеями, стоящими за W3. Только для того, чтобы признать, что сам по себе аргумент не имеет никакого смысла. Во-первых, в нашей

истории было много раз, когда приходилось ждать технологического прорыва, чтобы что-то изменить (например, телескоп). Более очевидный аргумент – наука. Тот факт, что кто-то перерезает кабели, не помешает общаться.

Давайте попробуем понять, как эти вещи работают, не заходя слишком далеко. Обмен электромагнитными импульсами – просто обмен нулями и единицами чем-то, способным их передавать (кстати, земля тоже на это способна, просто не очень удобна). Нельзя забывать, что код и электроны никем не контролируются. Они существуют как часть Вселенной. Изобретение телеграфа стало прорывом в этой области. Но возможность создания сетей не может быть отнята у кого-то, если только не отняты знания. Более того, сегодняшняя технология позволяет обмениваться сигналами другими способами: например, по радиочастотам, Wi-Fi и др.

Всё это показывает, что возможно создать «локальные ячеистые сети», которые соединены с другими сетями, не контролируются каким-либо субъектом, включая правительство. Это – вопрос знаний и фундаментальной науки. Вопрос одного шага, который отделяет от создания собственных физических сетей. Они уже существуют и используются. Вопрос только в том, а насколько широко? Но было время, когда большинство людей прилипли к Библии (не имея реальной способности читать её), вместо того чтобы понять, как свет от звёзд достигает Земли[48] и что Земля

[48] На самом деле сегодня живём во многом в эпоху высокотехнологичного

обладает доказанными и объяснимыми (с точки зрения науки) качествами.

Если возьмём эту информацию и доведём до современных технологий, то с помощью Wi-Fi, триангуляции или любой другой технологии построения сетей, включая ethernet (или любого другого способа разделения пропускной способности) и, очевидно, набора узлов, которые должны общаться друг с другом, сможем создать любые уникальные сети, то есть компьютеры – машины, которые могут считать (8 бит, 16 бит и т. д.). Если одна машина подключена к другой через кабель или антенну, она может передавать нули и единицы к другой машине. Это изображения цветов, цифр, строк, слов и т. д. Нам пришлось бы шифровать и расшифровывать данные. Убедиться, что они были приняты правильным аппаратом и т. д.

Звучит знакомо?

Конечно, так работает маршрутизация данных. Суть проста. Восстановление этого не требует больших усилий, как думали ранее. Более того – теперь кажется, что децентрализованные одноранговые сети не менее, но, возможно, даже более приспособлены к такой работе!

Средневековья (В. П.).

Больше, чем просто технология

Могу описать W3 следующим образом: это – следующий эволюционный шаг в развитии Паутины. Шаг, который уводит от централизации поисковых и социальных служб и от вещей, которые зависят от единой функциональной единицы (имеют центральный источник полномочий). Это шаг, который хочет, чтобы вовлечённые контрагенты и приложения общались друг с другом напрямую. По согласованию друг с другом: в то же время – быть мотивированным к такому поведению. И, как результат, добиться более безопасной маршрутизации данных и пакетов (обмен информацией) в сети.

Но это – технологическое описание. Текст составлен таким образом, чтобы могли думать и решать, может ли технология помочь выйти за пределы технических возможностей. Всё это – инструменты, позволяющие понять гораздо более крупные и важные вещи в жизни. Инновации и ответственность. *Что мир, свободный от цензуры, принуждения и коррупции, уже существует*. Нам просто нужно потянуться к нему.

Последний вопрос, который остаётся без ответа: когда именно всё это произойдёт?

Что ж, позвольте дважды разочаровать в одном абзаце. Во-первых, он уже функционирует. Это инфраструктурный

этап. Проблема (фича, но не баг) в том, что мир живёт в эпоху информации и люди всюду видят её. И это хорошо. Но когда что-то видите – хотите это почувствовать и сразу же попробовать. К сожалению, сейчас это не так для пользователей технически не продвинутых[49]. Второе – нужно подождать ещё пару лет, прежде чем «все эти штуки» перейдут на прикладной уровень. Более того, это, скорее всего, не приведёт к массовому внедрению. Но, может быть, через 5—10 лет увидим, как массы будут использовать некоторые основные применения коммуникационной технологии W3.

[49] Впрочем, искренне надеемся, что данная книга исправит и сей аспект (прим. В. П.).

Глава III. Краткие итоги истории

Умные устройства всё чаще порождают глупых людей.
Menaskop

Глава написана криптоэнтузиастом и создателем Synergis В. Поповым (aka Menaskop).

Web 3.0 не родился с первого раза: строго говоря, впервые о нём заговорили ещё в 2007 году, но на тот момент не было ясно, как именно соединить всё то, чем W3 должен отличаться. И всё же ряд наследственных звеньев – существуют до сих пор. Другой вопрос – можно ли их массово применять ныне?

Скажем, RDF (Resource Description Framework) – целая модель для представления любых, в том числе – и метаданных. Цитирую: «RDF является стандартом для кодирования в семантическом вебе (Semantic Web). Благодаря семантическому вебу компьютерные программы могут использовать возрастающие объёмы структурированных данных, распределённо и децентрализованно рассеянные по Сети в настоящее время. RDF представляет собой абстрактную модель, обеспечивающую способ разбиения знаний на дискретные части».

Зачем? В первую очередь для того, чтобы процесс получения знаний стал… децентрализованным: удивительно, как человечеству приходится раз за разом открывать и переоткрывать очевидные истины, но это факт[50], и его нужно принимать во внимание.

Ещё три звена наследственности – DAML, OIL и OWL. Кратко и о них: первый расшифровывается как язык моделирования цифровых активов; второй – онтологический уровень выводов; третий – язык веб-онтологии. При этом онтология в данном случае понимается не в философском, а в сугубо прикладном значении как «попытка всеобъемлющей и подробной формализации некоторой области знаний с помощью концептуальной схемы».

OWL является своего рода переработкой OIL и DAML[51], и в его случае вновь возвращаемся к Uniform Resource Identifier, то есть унифицированному идентификатору ресурса, поскольку OWL способен описать что угодно в модели «объект-свойство».

Но всё это прекрасно, пока не возвращаемся к тому, что указанные стандарты описаны и созданы W3C, а их практическое применение вне описанных концепций W3 – скорее

---

[50] В уже указанной ссылке https://ru.bmstu.wiki/RDF_(Resource_Description_Framework) есть дополнительные источники для изучения. Или можно обратиться к стандартной Wiki – https://ru.wikipedia.org/wiki/Resource_Description_Framework.

[51] Впрочем, ещё можно упомянуть и язык запросов поиска связанных данных – SPARQL.

теоретическое.

Другое же достижение прошлых лет – граф знаний, добавленный в Google в 2012 году. Подробное описание можно изучить по ссылке – во всё той же Википедии, но хочется отдельно акцентироваться на следующих моментах:

– Опыт – прекрасное подспорье для развития инноваций, но ещё важнее – контекст использования: если просто принять кем-то заданные стандарты, то это не решит основной проблемы – не сможем создать нескольких независимых (ещё точнее – положительно взаимозависимых) точек развития, как это есть на сегодня, когда IoT, AI / big data, ДРС развиваются и стандартизируются, но при этом не имеют уже столь сильной зависимости от гигантов экономики: включая и «железные»[52] решения, поскольку open source сначала овладел ПО, а теперь перешёл и к оборудованию.

– Не стоит, с другой стороны, пытаться избавиться от субъекта как такового (ошибка тех, кто считает, что только (!) код – закон): всё же технологии создаются для человека, а не человек – часть технологии. Мысль звучит банально после «Матрицы», но, к сожалению, как показано в приложении №1 – всё ещё актуальная.

– Безусловно, можно вспомнить, откуда именно пошло понятие «семантический веб»[53], но в рамках настоящей кни-

---

[52] Один из примеров – https://habr.com/ru/post/157527/. Почему это так важно? Читайте здесь.

[53] Если интересно – всегда можете изучить в материале А. Болдачёва «Web 3.0,

ги важно несколько иное: «Семантическая паутина изначально представлялась исключительно как надстройка над существующим Интернетом (тогда ещё, естественно, web 1.0). То есть в качестве носителя семантически размеченных данных мыслились обычные страницы и другой контент миллионов разношёрстных веб-сайтов. Предлагалось каждый объект – каждую веб-страницу, файл, описание офлайн-объекта на веб-странице – наделить унифицированным идентификатором и, используя эти ссылки, объединить весь сетевой контент в единую семантическую сеть… Так вот, даже этого знания о планах плетения семантической паутины уже достаточно, чтобы понять их бесперспективность. Очевидно, что самым слабым звеном в этом проекте является использование в качестве его основы обычных веб-страниц».

И именно поэтому, с одной стороны, важен процесс децентрализации, а с другой – изменение парадигмы представления, поиска и развёртывания информации внутри Сети нового поколения.

Выскажу по этому поводу ряд значимых соображений.

или Жизнь без сайтов» по адресу https://vc.ru/future/81683-web-3-0-ili-zhizn-bez-saytov.

Парадокс ничьей и ИИ

Недавно в очередной раз сражался с алгоритмом, играя в шашки на смартфоне, и обнаружил[54] проблему, которая давно витала где-то, но не выкристаллизовывалась.

Дело в том, что скрипты игры были настроены так, чтобы побеждать, когда же речь шла о явной ничьей – начался изматывающий процесс: однотипные ходы по кругу. И уже через сорок-пятьдесят таких итераций мой мозг устал, а вот компьютеру было всё равно: на то он и компьютер?

И в этот момент явственно ощутил, что таких аспектов, когда машине безразлично, а человек должен мобилизовать всю свою выдержку, терпение и прочие сопутствующие качества, будет крайне много.

Взять хотя бы Siri или Алису: не раз приходилось слышать, как они заблуждаются насчёт речевых обращений своих «хозяев». И в итоге – раздражение. Но как бы ни извинялись помощницы – они не испытывают эмоций. Никаких. Поэтому приходится констатировать, что в подавляющем большинстве случаев при ничьей у роботов возникает явное преимущество.

При чём тут W3?

Если принять во внимание глобальную систему репутации (см. ниже), где объект и субъект изначально равны, то

[54] Данный материал был опубликован В. П. изначально в рамках статьи.

получим, что на самом деле ситуаций подобного паритета будет с каждым годом всё меньше и меньше, за счёт как количественного увеличения устройств (один только рынок IoT может насчитывать 30 млрд устройств при 8 млрд людей на планете), так и качественного, поскольку нейронные сети обучаются ежесекундно.

Но это далеко не единственный парадокс внутри W3 – рассмотрим и другие…

Свобода: смарт-контракт и GDPR-крепостные

Недавно в Сети зашёл спор о том, что смарт-контракт есть ограничение свободы. Прежде чем развёрнуто ответить на тезис, а также вывести от него логическую связку к цифровому рабству, создаваемому через тестовый документ под вязкой аббревиатурой GDPR, обратимся к диаграммам Эйлера – два непересекающихся круга: обычно люди примерно так представляют уровни свободы индивидуумов, но на самом деле в 99% случаев выглядит это иначе – как круги пересекающиеся, и довольно плотно.

То есть из уровней «зависимость – независимость – взаимозависимость» высшим всегда остаётся последний. Поэтому взаимное ограничение свободы на основе полученного волеизъявления и есть то высшее благо, за которое должен бороться всякий мыслящий человек в эпоху тотального перехода к регрессии формаций по К. Марксу[55].

Отсюда и возникает набор следующих условий:

– Смарт-контракт как определённая степень взаимных ограничений ради достижения общего результата (ограни-

[55] То есть не от рабства к феодализму, капитализму и от него далее к коммунизму, а в эпоху цифрового рабовладельческого строя, где условно-свободным может быть лишь аватар виртуального мира, а вероятно – и он будет под игом, как это показано в известном сериале «Чёрное зеркало».

чения не имеют в данном контексте негативного нарратива) достигается через обоюдную договорённость сторон и никак иначе: проще говоря, «спущенные сверху» умные контракты противоречат собственной природе, как и акцептованные в одностороннем порядке.

– Кроме того, цель смарт-контракта не есть ограничение свободы субъекта (или объекта), а именно автоматизация конкретных действий (в случае DAO – набор расширяется, в случае Dapps'ов – масштаб увеличивается до глобального), то есть тем самым создаются условия для устранения рутинных операций для, что крайне важно (!), высвобождения времени под социальные транзакции более высокого уровня – творческих и подобных. Но никак не наоборот!

– И именно по этой причине smart-contract'ы, созданные[56] вне публичных блокчейнов или dag-подобных решений, не могут гарантировать ни собственного исполнения, ни взаимозависимости связанных через себя субъектов/объектов.

И в этом смысле W3 – не идеальное, возможно, но вполне допустимое решение, где каждая цепочка взаимосвязей может быть продиктована разной мотивацией и мотиваторами (будь то токены, социально полезная деятельность или что-

[56] На самом деле для меня близка парадигма, что разработчик-будущего (условно в «Тени завтрашнего солнца» называю его «модельер») создаёт некие бизнес- или же модели быта, а уже искусственный интеллект пишет собственно смарт-контракт (В. П.).

то ещё).

Централизация и Web 3.0: коротко

Опять же, о полезности споров (но не дискуссий). Намедни, общаясь с одним из ведущих разработчиков, выявил два важных тезиса:

– Сайт может быть[57] централизован, но отдать юзерам «управление» своим пространством.

– Единая авторизация[58] предполагает и единый ключ

---

[57] Приведу верное замечание А. Пискунова: «Сайт в текущей ситуации **всегда** централизован: кто владеет доменом – может указать сервер, который будет выдаваться посетителям; кто владеет сервером – может указать скрипты/файлы для взаимодействия с пользователями; кто владеет скриптами/файлами (имеет к ним доступ) – может менять содержимое и выполнять js-код у посетителей на компьютере; пользование сайтом – акт доверия: во-первых, владельцу домена; во-вторых, владельцу сервера; в-третьих, владельцу файлов. Не бывает децентрализованных сайтов „пока“. Бывают сайты, где открыт код, который можно изучить, где можно посмотреть потоки данных и решить для себя: заслуживают ли они доверия? Сайты/скрипты могут отдать часть ресурсов/данных на управление пользователям – и всё! Дать доступ к файлам/скриптам – не могут, так как нельзя доверять их содержимому, а если дать „управлять“ файлами – то это дыра (как загрузка вредоносных скриптов и взлом изнутри уже)». Всё это так, скажу я (В. П.), но выше идёт речь именно о модели, когда условный сайт становится таким же открытым вместилищем, как и любая ДРС. Методология создания таких «сайтов» представляет собой совокупность практик совместных репозиториев (на Github или других ресурсах), построения p2p-сетей формата TOR или торрентов, а равно и консенсусные решения внутри ДРС.

[58] Опять же – адресую к комментарию А. Пискунова: «Единая авторизация предполагает и единый ключ шифрования данных для взаимодействия с другими участниками». Не понял (этот момент): что, если Гугл решит авторизовать другого пользователя от твоего имени? Это акт доверия: исключить «доверие»

шифрования данных для взаимодействия с другими участника.

Действительно, такой подход имеет место быть, но как он соотносится со степенями свободы, выраженными в разнопорядковых цифровых отпечатках личности?

Никак.

Потому как кастомизация интерфейса на сегодня доступ-

можно лишь при использовании распределённых систем для получения публичного ключа, чтобы провести проверку действия, когда юзеры будут подписывать своим ключом все действия – только тогда можно убедиться, что перед тобой нужный юзер: юзер должен понимать – что ОН владелец «авторизации». Потерял ключ = потерял личину на сайте, поэтому не понимаю «единая авторизация предполагает и единый ключ шифрования данных» для взаимодействия с другими участника. Возможно, это объяснено не под тем углом: (как) говорил, единая авторизация возможна в том случае, если есть провайдер публичных личин (пространства имён) и ты можешь проверить там публичный ключ (ключ подписи). Тогда любой сайт сможет обратиться к доверительному сервису с доступом к данным из того или иного блокчейна, а может, у него своя нода для доступа к эфиру. Получить проверку – что перед ним тот аккаунт, который «доказал», что это он, с помощью криптографии. Мне не нравится предложение «единая авторизация предполагает и единый ключ шифрования данных для взаимодействия с другими участниками». Оно (несколько) путает: ключ шифрования – всё-таки другая вещь, не ключ для криптографической валидации подписи. Есть криптографические методы для нахождения shared key между двумя ключами, когда каждый участник может с помощью публичного ключа собеседника и своего приватного ключа получить shared key, который уже можно использовать для шифрования сообщений. Этот shared key получается одинаковый у обоих собеседников: никто другой не может получить его, для этого нужно знать один из приватных ключей двух собеседников. Опять же, всё верно (с моей точки зрения – В. П.), но смысл фразы сводится к тому, что сегодня – эпоха мультиблокчейнов, а за ней необходимым образом следует эпоха мультихранилищ ключей авторизации/шифрования/валидации, но пока, конечно же, это лишь гипотеза.

на и в Web 2.0, а что касается единой авторизации, то это – техническая «надстройка» над Oauth 2.0 и аналогами. При этом всегда возникает вопрос «рубильника», потому как никакого распределения ответственности de facto не существует и администратор самостоятельно определяет правила, когда и кто имеет право на те или иные действия. Банальные чёрные списки (читай – антисписок Шиндлера).

Но важнее другое: никакая децентрализованная система не допускает ограничений для централизованных система apriori. Тогда как обратное – вполне объяснимо и существует сплошь и рядом.

То есть при доминирующем положении в Web 3.0 p2p-систем нового уровня (нечто подобное сейчас формируется в экосистеме BitTorent & Tron) сохраняется и возможность многомерного распределения, включая и классические, клиент-серверные архитектуры.

В противном же случае цифровая зависимость будет уже не красивым эпитетом, а реальностью, которая вкупе с VR/AR-действительностью поглотит нас в ближайшую четверть века. Нас – как объекты!

Дапсы и локальные глобальные сети – находка архитектуры Web 3.0

Dapps'ы (децентрализованные приложения) широко пиарятся ныне, не хуже ICO в 2016—2017 гг., но чем именно они так хороши? Задумывались ли вы, что сама по себе архитектура дапсов позволяет им быть фактически бесконечно вложенными?[59]

Что имеем сегодня: есть, допустим, Facebook & Instagram – взаимозависимые приложения. Но их вложенность минимальна: можно делать перепосты, есть ретаргетинг, указание профиля и всё в этом духе. Для пользователя всё равно два разных сервиса. Даже банальные юридические формальности – разные.

С dapps'ами всё не так: в них имеем возможность не только вертикального, но и горизонтального масштабирования, за счёт связок decentralized applications решений. Но и это не всё.

Как помним, W3, в отличие от создаваемой псевдодецентрализованной системы от корпораций (почитайте про blockchain от Facebook и криптовалюту JP Morgan), даёт пользователю возможность самостоятельно генерировать

[59] Впервые данная подглава была описана в виде отдельной статьи и опубликована в онлайн-журнале coinmedia.

для нужной степени вложенности свой цифровой отпечаток и распоряжаться им по временному, количественному и прочим измеряемым критериям.

Например, псевдоним Menaskop: сегодня ник есть на том же Facebook'е и Хабре, но что могу? На Хабре чуть больше: помимо лайков/плюсов можно заработать карму и рейтинг. Но как насчёт срока действия аккаунта? Либо удаляюсь и теряю всё (к тому же – более одного раза невозможно даже обнуление на Хабре, а на FB его и вовсе нет), либо принимаю правила и работаю «как есть».

Но это ведь мои (!) данные: даже уже GDPR (General Data Protection Regulation, правила защиты персональных данных, принятые в Европе) и ФЗ №152 в РФ приняли и подтвердили, что мои. Но только на бумаге: de facto всё хуже: корпорации зарабатывают на этом миллиарды, я – ничего, кроме набившей оскомину рекламы. Подписки ещё создадут прецеденты цифровой нетерпимости, но пока все упорно делают вид, что толерантны. Донельзя!

И вот здесь помогают цифровые слепки W3: сам определяю, когда и сколько хочу взаимодействовать с конкретным сервисом.

Первые шаги к этому – сервисы децентрализованной идентификации, социального майнинга (SportCoin, Bitradio, Brave), медиаблокчейны (Steem, Golos[60], Decent, UOS). Соответственно, в любой момент времени могу:

[60] Есть, скажем, мастер-ключ, ключ для постинга и т. д.

– ограничить ширину/глубину взаимодействия конкретного цифрового слепка;

– установить временной лимит (простейший пример – через смарт-контракт);

– удалить/восстановить конкретный слепок.

Таким образом, Menaskop всегда будет в конкретном децентрализованном или распределённом приложении, но ровно по тем параметрам, которые задам ему я. Кроме того, для dapps'ов на Ethereum будет, например, слепок с полномочиями из набора №1 – предельно широкий, для EOS – из набора №3, с минимальными полномочиями, а для Sia – №2. И, соответственно, связки Ethereum + EOS + Sia начнут работать от большего к меньшему.

Схема взаимодействия «цифрового слепка» пользовательских данных в Dapps в различных блокчейнах: *что это даёт*?

Помимо правильной с архитектурной точки зрения системы саморегулирования – ещё и практическую схему неразрывной взаимосвязи принципов децентрализации, анонимности, открытости и транзакционной репутации.

А что дают эти принципы?

Во-первых, главное – *свободный* Интернет. Хотим этого или нет, но сегодня Сеть[61] стала несвободной для большинства. Да, есть те, кто ежедневно отстаивает общие интере-

[61] Читай подробней в приложении №1, но здесь напомню про Великую огненную стену в Китае aka государственный Firewall и автономный Рунет (В. П.).

сы, но пока общий процент минимален. W3 вкупе с другими тенденциями позволит этот процент удесятерить.

Во-вторых, подобный формат создаёт безграничные возможности для предпринимателей. Можно:

– объединять усилия и достигать синергии уже не на словах, а на деле: истинные DAO (на основе методик «бирюзовых организаций») – следующий шаг вперёд;

– придумывать новые общественные решения, невозможные в заданной сейчас системе координат и в принципе, и в конкретике;

– наконец, не бояться отключения со стороны провайдера, потому как они способны создавать ГЛС – глобальные локальные сети.

Wi-Fi Aware, предрасположенность 5G к мэш-сетям (как и bluetooth-стандарта), развитие инфраструктуры для IPFS/Filecoin[62] – следующий[63] шаг, которого так не хватало: покрыть физический уровень альтернативными (Интернету) сетями – задача ближайшего десятилетия.

И в этом смысле W3 – уже не логичное продолжение W2, но и модель противостояния тем негативным тенденциям, которые заложены в современном социуме: будь то управляемые цветные революции, законы о едином цифровом про-

---

[62] В этом смысле – полезно следить не только за новостями, но и конкретными личностями: например – https://en.wikipedia.org/wiki/Juan_Benet_(computer_scientist).

[63] Кстати, подумайте и о технологии IPv6 именно с этой позиции.

филе гражданина или вовсе – мировой рейтинг, созданный по непонятным правилам непонятными структурами.

Глава IV. Web 3.0 – этап эволюции систем

Глава написана создателем децентрализованного объединения Synergis, писателем, философом, криптоэнтузиастом, анархистом, известным под ником Menaskop, Владимиром Поповым.

Опять эволюция?

Изначально эта часть появилась не как элемент книги, но как предварительные исследования по проекту iTerra. Затем, уже в полной переработке – была вшита в общую ткань сего труда. И вот почему…

Дело в том, что, как только приступил к изучению W3, а было это в начале 2018 года, обнаружил, что всё, до чего бы ни дотрагивался взгляд, в той или иной степени является новым уровнем абстракции.

Допустим, языки программирования: изначально это был просто машинный код – отсюда эта сложная система 11001001000011111110110…, перфокарты и т. д. Затем появился ассемблер: первые хакеры, да и ныне живущие и придерживающиеся основ, отличались от обычных кодеров тем, что могли оптимизировать программы самыми нетривиальными[64] способами. Затем настала эпоха языков программирования высокого уровня[65]: то с победой ООП, то с возвратом к возможностям языков функциональных.

Но что же имеем сегодня?

Всё больше и больше технических специалистов понимают, что и в связи со сложностью существующих бизнес-

[64] Например, доводить до совершенства код, и так написанный в 10—12 строк.

[65] Подробней см. https://ru.wikipedia.org/wiki/История_языков_программирования.

и иных социальных процессов, а равно и ввиду постоянных модификаций самих языков, платформ, которые через них создаются, и всей инфраструктуры в целом, даже не паттернизация, а *моделирование* является следующим уровнем абстракции, который следует применять для оптимизации всё новых и новых автоматизируемых сущностей.

Но языки программирования – только начало: одна из сущностей.

Конец ознакомительного фрагмента.